UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE CIENCIAS Y SISTEMAS

MAESTRÍA EN GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

CICLO ACADÉMICO 2017- 2019

INFORME FINAL DE TESIS PARA OPTAR AL TÍTULO DE MÁSTER EN GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

"IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO DE EVENTOS DE SEGURIDAD EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA EMPRESA ADMINISTRADORA DE AEROPUERTOS INTERNACIONALES (EAAI)"

Elaborado por:

Ing. Diego Manuel Vega Amoretti #Carnet: 2017-0013M

Tutor: MSc. Ing. Reynaldo Antonio Castaño Umaña

Managua, Noviembre 2019.

DEDICATORIA

A DIOS

Por ser el autor de la vida, el único que me ha dado la salvación, protección, salud, fuerza, inteligencia, perseverancia y firmeza para mantenerme todo este tiempo en el camino correcto y bajo su gracia. A demás por ser el Señor que rige mi vida y a quien le debo todo lo que soy.

A mi Esposa

Por ser la ayuda incondicional que Dios me dio, por estar todas las noches a mi lado mientras trabaja o estudiaba. Por ser una mujer excepcional capaz de comprender y esperar pacientemente aun cuando el estrés o la fatiga me irritaban.

A mis Padres

A mi Padre Diego Manuel Vega Marín (qedp) quien fue un ejemplo de amor, superación y perseverancia. A mi Madre María Elena Amoretti por sé una mujer fuerte, amorosa, protectora y que también se sacrificó por darnos lo mejor. Gracias por haber hecho un buen trabajo conmigo y mis hermanos.

A mis Hermanos

A Marlon José Vega Amoretti y Jessee Elieth Vega Amoretti por creer siempre en mí, por darme ánimo para seguir adelante, por saber que siempre puedo contar con ustedes sin importar el tiempo o el espacio.

A mi Suegra

A Matilde Soriano Pastrana por estar siempre pendiente de mi salud, alimentación y apoyarme en todas las necesidades que tengo junto a mi esposa. Muchas Gracias.

A todos mis hermanos en Cristo de la Iglesia Puerta Del Cielo

Por estar pendientes preguntando ¿Cómo va la Tesis? y diciendo yo se que usted puede siga adelante. Muchas Gracias por sus oraciones y amistad.

AGRADECIMIENTOS

A mi maestro y tutor Msc. Ing. Reynaldo Antonio Castaño Umaña

Por haberme motivado todo el tiempo de la maestría a dar lo mejor de mí, por saber trasmitir conocimientos e inducir a buscar más de lo que nos brinda. Gracias por estar dispuesto a corregir todo lo que hago sin importar la hora. Gracias por su esfuerzo y dedicación.

A mi Jefe, Compañero y Amigo Msc. Ing. Juan Ernesto Aguilar Narváez

Por apoyarme durante todo el proceso de la maestría y brindarme siempre el apoyo para poder ingresar a la misma. Por estar a mi lado cuando le necesito sin importar hora, recursos o lugar; por ser siempre un apoyo para mi vida. Gracias por confiar y creer en mí.

A mi Gerente General Msc. Aleyda Molina

Por brindarme la confianza y oportunidad de ingresar a la universidad para perfeccionar mis conocimientos. Gracias por creer en mí, por apoyarme como persona y como responsable de la E.A.A.I.

RESUMEN DEL TEMA

Nuestro bello país Nicaragua hoy día empieza a surgir y verse más que un simple punto en el mapa. Los continuos desarrollos en todos los ámbitos hoy por hoy son más evidentes. En cuanto a la tecnología tampoco nos hemos quedado atrás. En este país hay mucho profesional capacitado, autodidacta y de gran conocimiento que está dispuesto a enfrentar retos y estar consientes del papel que juega dentro del desarrollo de la nación. Las tecnologías de la información y comunicación hoy son una realidad en nuestro diario vivir, más sin embargo muchos ignoran los riesgos, vulnerabilidades y amenazas a las que están expuestos. Cualquier persona puede decir que no tiene problemas y que está seguro con su información; pero solo basta un equipo (Router, punto de acceso inalámbrico) mal configurado o con vulnerabilidades conocidas de fábricas para que un tercero mal intencionado y sin escrúpulos utilice tú equipo para penetrar sistema o redes de otros.

El incremento de la actividad delictiva en el internet es evidente, no solo existen secuestros virtuales a nuestros equipos e información. Sino que estamos siendo participantes muchas veces sin saberlo de ataques de denegación de servicios distribuidos. Lo que con este desarrollo de tesis se pretende es enseñar y fomentar a toda empresa responsable como la correcta administración, correlación, almacenamiento y clasificación de los LOG (Registros de Seguridad de equipos). Se pretende desarrollar los elementos básicos para proveer una visibilidad completa de nuestra infraestructura tecnológica.

Con esta tesis podrán desarrollar bases solidas para instalar, configurar y administrar un sistema de monitoreo de eventos de seguridad por medio de un SIEM basado en código abierto. Se demostrará que con pocos recursos económicos podemos obtener grandes beneficios en materia de seguridad y rápida respuesta a los incidentes de seguridad que se presentan en nuestra infraestructura tecnológica.

ÍNDICE

Índice de imágenes

Índice de Tablas

1. INTRODUCCIÓN

La Empresa Administradora de Aeropuertos Internacionales (**EAAI**) es una entidad descentralizada del gobierno de la república de Nicaragua. Siendo un ente autónomo cuya función principal es administrar las terminales aéreas de Managua, terminal con pista alterna en Panchito, terminal de Corn Island, terminal de Bluefields, terminal de Puerto Cabezas (Bilwi), terminal de San Juan de Nicaragua y la terminal aérea la Paloma (Ubicada en la Isla de Ometepe). Además tiene como principales funciones en los distintos aeropuertos que administra brindar la logística, seguridad e infraestructura necesaria para que tanto las líneas aéreas, pasajeros, visitantes, arrendatarios, entidades de gobierno (INTUR[2], DGA[3], MAGFOR[4], MINSA[5], DID[6], POLICIA, TELCOR, ONA[7], INAC[8]) e ISP[9] puedan brindar o recibir servicios.

La misión de la EAAI[1] es facilitar los servicios de vuelos nacionales e internacionales y por ende las áreas administrativas por medio de la GTI[10] hacen uso de las tecnologías de la información para el procesamiento de sus datos contables y obligaciones con proveedores.

Para la EAAI[1] la seguridad de la información es uno de los principales elementos que se están tomando en cuenta por los altos directivos de la empresa. Esta importancia que han tomado en incrementar la seguridad de la información se puede observar en la inversión de activos tecnológico que salvaguardan la seguridad, integridad y disponibilidad de la información. La EAAI está consciente de las vulnerabilidades y amenazas presentes en los SI[11].

[1]**EAAI:** *Empresa Administradora de Aeropuertos Internacionales.*
[2]**INTUR:** *Instituto Nicaragüense de Turismo.*
[3]**DGA:** *Dirección General de Aduanas.*
[4]**MAGFOR:** *Ministerio Agropecuario y Forestal.*
[5]**MINSA:** *Ministerio de Salud.*
[6]**DID:** *Dirección de Información para la Defensa.*
[7]**ONA:** *Organismo Nacional de Acreditación.*
[8]**INAC:** *Instituto Nicaragüense de Aeronáutica Civil.*
[9]**ISP:** *Acrónimo de Internet Service Provider, en español proveedores de servicios de Internet.*
[10]**GTI:** *Gerencia de Tecnología de la Información.*
[11]**SI:** *Sistemas de Información*

Según el análisis de riegos se determinó que existen vulnerabilidades en los sistemas de información que pueden ser explotadas por el personal de la empresa (Trabajadores permanentes o temporales) o por agentes externos (Usurpadores de identidad, Ladrones de cuello blanco, Hackers). La probabilidad de ocurrencia de que una vulnerabilidad pueda ser explotada en las empresas aumentan con las nuevas tecnologías y la evolución de los diferentes tipos de software tanto para sistemas operativos, software especializados de gestión de bases de datos, sitios web, servicios de mensajería, correo electrónico y compras en línea. Para hacer frente a los retos de seguridad actuales la EAAI[12] utiliza herramientas de hardware y software que se encargan de salvaguardar la información de la empresa. A demás se utilizan aspectos básicos como el uso de configuraciones que permitan el endurecimiento de equipos de la infraestructura de red y la implementación de certificados de seguridad SSL[13] o TLS[14] para proteger el canal de comunicación de la información; sin embargo esto no es suficiente. Aunque el ambiente de cada organización es muy particular existen prácticas que deberían adoptarse en las políticas internas que utilizan las empresas para asegurar su principal activo que es la información. En este ámbito la EAA[12] ha venido invirtiendo en materia de seguridad permitiendo una red interna en su terminal de Managua de más de 400 dispositivos interconectados (Servidores, Routers, Switches, Impresoras, Computadores de escritorios y portátiles) y posee además conexiones a las redes internas de 4 terminales aéreas ubicadas en la costa Caribe.

El presente trabajo se desarrolla con el propósito de contribuir a la EAAI[12] a tener visibilidad de los eventos que ocurren en la infraestructura tecnológica, aprovechando que el equipamiento genera registros que permiten la identificación de ataques, comportamientos anómalos de parte de usuarios y eventos que pueden perjudicar la operatividad de los servicios y/o perdida de información sensible.

[12] **EAAI:** *Empresa Administradora de Aeropuertos Internacionales*
[13] **SSL:** *Secure Sockets Layer*; en español capa de puertos seguros)
[14] **TLS:** *Transport Layer Security*; en español seguridad de la capa de transporte

Durante todo el desarrollo del presente trabajo se podrá observar el proceso de identificación y selección del software SIEM[15] a utilizar; se identificará del mercado actual tanto las características comparativas como los costos asociados y sus beneficios de un grupo reducido de software SIEM[15]; esto de acuerdo a los software más destacados en el cuadrante Mágico de Gartner. A demás se analizarán las necesidades de procesamiento y almacenamiento de la empresa con el objeto de recomendar la solución más factible según las necesidades. Para la ejecución de este proyecto se solicitará a la GTI[16] de la EAAI[17] la autorización para implementar por un periodo corto de tiempo al menos dos soluciones SIEM[15].

Al finalizar este trabajo se hará recomendación de la solución más efectiva y se proveerá una solución alternativa al implementar una prueba de concepto de dos SIEM[15]. Dentro de los resultados que se obtendrán está la documentación de todo el proceso de configuración y operación del software SIEM[15]. A demás se realizarán pruebas de ataques a la infraestructura tecnológica de la EAAI[17] y se podrá observar la visibilidad que brinda el integrar todos los registros de seguridad en un solo software capaz de correlacionar y crear reglas que permitan alertar al personal de los ataques que se estén produciendo en tiempo real.

[15] **SIEM:** Security Information and Event Management en español conocido como Sistema de Gestión de Eventos de Seguridad de la Información.
[16] **GTI:** *Gerencia de Tecnología de la Información.*
[17] **EAAI:** *Empresa Administradora de Aeropuertos Internacionales.*

2. ANTECEDENTES (PLANTEAMIENTO DEL PROBLEMA)

La Empresa Administradora de Aeropuertos Internacionales (**EAAI**) en su continua etapa de transformaciones está preocupada por mantenerse con niveles de servicios óptimos que garanticen la competitividad a nivel internacional. Para mantener su alto desempeño la estructura interna de la empresa tiene dividida las tareas del área de operaciones aeronáuticas y todas sus dependencias tecnológicas requeridas para las operaciones diarias; y las áreas que son administrativas con su respectiva área de tecnología de la información.

Hace 15 años la empresa apenas tenía una red de unos 30 computadores y sus sistemas se basaban en gestores de base de datos antiguos que operaban en modo texto. En la actualidad existen más de 400 dispositivos de red conectados a nivel LAN[18] que generan un gran volumen de tráfico e información y existen conexiones VPN[19] de sitio a las terminales de la costa Caribe (Bluefields, Corn Island, Puerto Cabezas) y en la Isla de Ometepe. Toda la información generada por equipos de comunicaciones, computadores y servidores debe ser adecuadamente gestionada y utilizada como un elemento importante durante la toma de decisiones y el monitoreo de los equipos de red. La seguridad de la información es atendida por el área de Infraestructura de Redes y Administración de Base de Datos que pertenece a la Gerencia de Tecnologías de la Información.

[18] **LAN:** Local Area Network, en español Red de Área Local.
[19] **VPN:** Virtual Private Network, en español Red Privada Virtual.

Uno de los principales problemas que actualmente enfrenta la EAAI[20] en materia de seguridad es cómo gestionar con el volumen disperso de información generado por los diferentes equipos de seguridad (Switches, Routers, UTM[21], Administrador de Ancho de banda) y Servidores; además del hecho que las terminales aéreas de la Costa Caribe no poseen un sistema de monitoreo de tráfico en tiempo real que enlace con el sistema de monitoreo de red de Managua. Actualmente el tráfico entre las terminales es transmitido vía VPN[22] pero el tráfico de internet es administrado por el Router local a cada terminal sin almacenar los registros de alertas de tráficos maliciosos en esas redes.

En la terminal de Managua se posee equipos de seguridad que brindan monitoreo del tráfico de la red y los almacenan en un servidor pero esto se realiza de forma manual en cuanto a las alertas y alarmas que se generan. La EAAI[20] con el pasar del tiempo ha venido intentando resolver los problemas de administración de los registros de seguridad de los equipos. Se han instalado varios software gratuitos de gestión de LOG[23] pero aun resulta muy difícil poder reconocer cuando los registros que ingresan de diversos equipos están indicando que son ataques los que se están efectuando. A demás ninguno de los software de gestión de LOG[23] era capaz de enviar alertas y de correlacionar eventos de seguridad.

En general el problema de administración existente se puede observar en la **Figura No1.** Diagrama Causa Efecto - Problemas EAAI.

[20]**EAAI:** Empresa Administradora de Aeropuertos Internacionales.
[21]***UTM:*** Unified threat management; en español Gestión unificada de amenazas.
[22]***VPN:*** Virtual Private Network; en español red privada virtual.
[23]**LOG*:*** *Registro de seguridad o Traza de auditoría de los eventos*

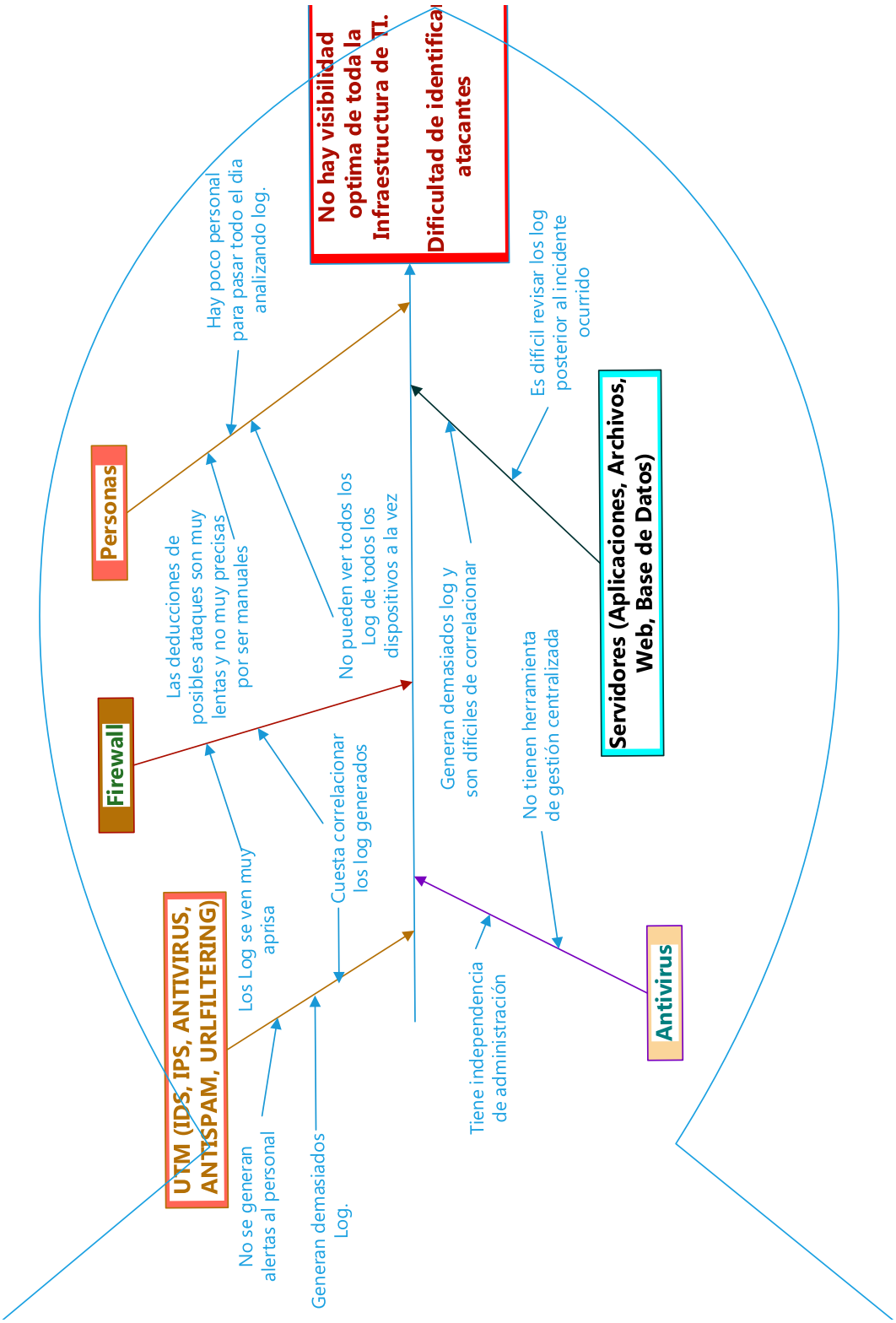


Figura No 1. Diagrama Causa Efecto- Problemas EAAI (Desarrollo propio)

Se muestra la complejidad de administración de todos los registros de eventos de todos los dispositivos de seguridad, red y servidores. A demás se observa que no existe un elemento que proporcione visibilidad en la infraestructura.

3. JUSTIFICACIÓN

Para la EAAI[24], administrar todos los componentes activos de una infraestructura de red en materia de seguridad es una ardua labor. Si le suman a la compleja administración la falta de visibilidad y de alertas automatizadas que detecten en tiempo real los ataques y comportamientos anómalos que pueden presentarse en las infraestructuras tecnológicas de la EAAI[24] tendrán un impacto adverso a la seguridad de la empresa. La EAAI[24] se posee un gran volumen de datos que generan los equipos de seguridad que no han podido ser gestionado de forma adecuada. Estos registros de seguridad se analizan de forma manual produciendo dificultad para entender lo que está ocurriendo en la infraestructura de red y por ende existe mayor probabilidad de no poder detectar a tiempo un patrón de ataque de forma detallada.

Para tener mayor visibilidad y control de la infraestructura de red la EAAI[24] requiere establecer las bases que permitan gestionar de forma centralizada toda la información provista por los distintos controles (Dispositivos de la infraestructura de red). Toda esta gestión centralizada es el tema a desarrollar mediante la implementación de una herramienta especializada de software SIEM[24]. Uno de los beneficios de la EAAI[24] con el SIEM[24] es que podrá integrar y correlacionar toda la información de los registros de equipos de comunicaciones, seguridad perimetral y servidores obteniendo una visibilidad completa de la infraestructura de red. Con la visibilidad y correlación de eventos obtenida por medio del SIEM[25] se podrá en tiempo real obtener la información de todos los equipos seleccionados y con todos los registros de seguridad almacenados en un solo depósito de datos permitirá un análisis de lo que está ocurriendo en la red y brindará la posibilidad de efectuar auditorias informáticas. Para la EAAI[24] una solución SIEM[25] no es solo un elemento de seguridad y cumplimiento de TI[26], sino que garantiza un mayor nivel de protección de los datos ya que al contar con una solución SIEM[25] los administradores de servicios y seguridad podrán detectar en tiempo real posibles ataques a la infraestructura.

[24] ***EAAI:*** *Empresa Administradora de Aeropuertos Internacionales*
[25] **SIEM:** Security Information and Event Management en español conocido como Sistema de Gestión de Eventos de Seguridad de la Información.
[26] **TI:** *Tecnologías de la Información.*

4. OBJETIVOS (GENERAL Y ESPECÍFICOS)

OBJETIVO GENERAL:

- Optimizar los mecanismos de monitoreo de eventos de seguridad en la infraestructura tecnológica y de servicios de la EAAI[27].

OBJETIVOS ESPECÍFICOS

- ✓ Realizar análisis técnico de las trazas de auditoría de eventos generadas por los recursos y protocolos de comunicación empleados en la infraestructura de seguridad y servicios tecnológicos implementados en la EAAI[27].
- ✓ Efectuar una comparación de las diferentes soluciones de SIEM[28], que permitan integrar y correlacionar los eventos generados por la infraestructura tecnológica de la EAAI[27].
- ✓ Definir el modelo de monitoreo y gestión de eventos de seguridad de la EAAI[27].
- ✓ Definir los costos asociados a la implementación, operación, mantenimiento y soporte del SIEM[28].
- ✓ Determinar la efectividad del sistema de gestión de eventos de seguridad, mediante la simulación de ataques informáticos a la infraestructura de servicios tecnológicos.

[27] ***EAAI:*** *Empresa Administradora de Aeropuertos Internacionales*
[28] **SIEM:** Security Information and Event Management en español conocido como Sistema de Gestión de Eventos de Seguridad de la Información.

5. MARCO TEÓRICO

5.1. INFORMACIÓN

Según (iso27000.es, 2018) se entiende por información "todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración." La **Figura No.2** Información según ISO27000 muestra de forma gráfica que la información es procesada y obtenida mediante distintas fuentes de datos pero el resultado final es el almacenamiento y resguardo de la misma.

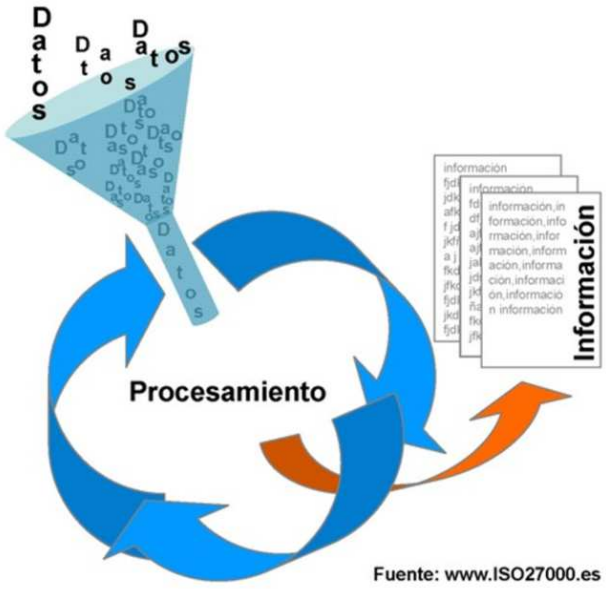


Figura No 2. Información según ISO27000

5.2. SEGURIDAD DE LA INFORMACIÓN

Durante las últimas décadas mantener segura la información de las empresas ha venido a ser una ardua tarea que no solo requiere de gran inversión económica en cuanto a infraestructuras de redes y equipos de seguridad sino que la parte humana debe de ser igualmente capacitada y debe estar consciente de la fragilidad de los recursos que está administrando. Muchas empresas han sido víctimas de ataques cibernéticos, piratería, phishing[29], malware[30] y otro tipo de violaciones o incidentes de seguridad que aún muchos de ellos no están conscientes de haber sido expuestos.

¿Qué es seguridad de la información?

- La seguridad de la información según (Wikipedia.org (Seguridad de la Información), 2018) "es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma"
- Según (iso27000.es, 2018) La seguridad de la información consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Por las definiciones anteriores se concluye que la seguridad de la información son un conjunto de normas, procedimientos, mecanismos y controles que garantizan el resguardo o protección de la información de las organizaciones y que preservan para ese efecto la triada de la seguridad (confidencialidad, integridad y disponibilidad)

[29] **Phishing**: Suplantación de Identidad.
[30] **Malware:** Del Inglés Malicious Software, en español Programa Malicioso.

5.2.1. PROPIEDADES DE LA INFORMACIÓN

En términos de seguridad de la información para que los datos o la información personal de una organización cumplan unos estándares de seguridad adecuados debe contener las tres propiedades mostradas en la **Figura No.3** Propiedades de la información.

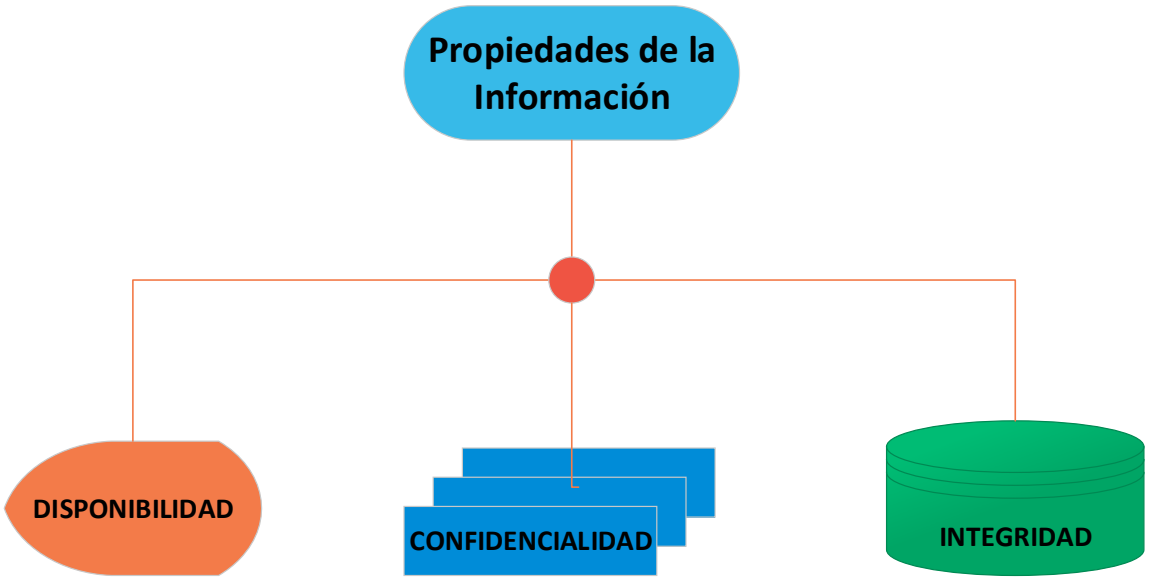


Figura No 3. Propiedades de la información (Adaptada de Chicano Tejada E., 2014, pág. 10, Propiedades de seguridad informática)

Según (firma-e.com, 2014) se define esta triada de la seguridad o propiedades de la seguridad de la información como:

Integridad: El diccionario define el término como "estado de lo que está completo o tiene todas sus partes". La integridad hace referencia a la cualidad de la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros. Esta integridad se pierde cuando la información se modifica o cuando parte de ella se elimina, y una gran garantía para mantenerla intacta es la firma digital. Un aspecto relacionado con la integridad es la **autentificación**; por autentificación se entiende como la cualidad que permite identificar al generador de la información y que se logra con los correctos

accesos de usuario y con otros sistemas como la recientemente mencionada firma electrónica. Para algunos, incluso, la autentificación sería el “cuarto pilar” de la Seguridad de la Información.

Confidencialidad: Por confidencialidad entendemos la cualidad de la información para no ser divulgada a personas o sistemas no autorizados. Se trata básicamente de la propiedad por la que esa información solo resultará accesible con la debida y comprobada autorización. La confidencialidad se pierde haciendo caso omiso a las recomendaciones de seguridad o no implantando un sistema adecuado; así, cuando compartimos equipos sin eliminar las contraseñas, olvidamos cerrar nuestro usuario, tiramos un disco duro sin borrar antes sus datos o no ciframos los datos de manera adecuada, la información deja de ser confidencial y entramos, digamos, en una zona de alto riesgo.

Disponibilidad: El tercer y último pilar de la Seguridad de la Información es la disponibilidad, y es posiblemente el término que menos apreciaciones requiere. Por disponible entendemos aquella información a la que podemos acceder cuando la necesitamos a través de los canales adecuados siguiendo los procesos correctos. Esta característica, la disponibilidad, puede en ocasiones chocar frontalmente con la confidencialidad, ya que un cifrado complejo o un sistema de archivado más estricto puede convertir la información en algo poco accesible, por lo que no se trata en absoluto de un punto menor y marca en gran medida el buen hacer del responsable de la seguridad de la información de la empresa u organización.

5.2.2. INCIDENTES DE SEGURIDAD

Según (Chicano Tejada, 2014, pág. 10) “un incidente de seguridad es cualquier evento que puede afectar a la integridad, confidencialidad y disponibilidad de la información. En otras palabras, y atendiendo a la norma ISO[31] 27001:2005, un incidente de seguridad es un evento no deseado o no esperado que puede comprometer significativamente las operaciones de negocio y amenazar la seguridad de la información.”

En la actualidad muchas empresas están empezando a preocuparse más por entender que tipo de vulnerabilidades tienen y a que riesgos están expuestos. Esta preocupación viene generando conciencia de la forma en que las organizaciones están gestionando la seguridad de la información y como están entendiendo y procesando los incidentes de seguridad que se estén generando en la empresa.

[31] **ISO:** Del *International Organization for Standardization, en español Organización Internacional de Normalización/estandarización.*

5.2.3. TIPOS DE INCIDENDES DE SEGURIDAD

Los tipos de incidentes según (Chicano Tejada, 2014, págs. 11-12) por ser muchos podrían tener la siguiente clasificación:

- ✓ Accesos no autorizados.
- ✓ Código malicioso o malware
- ✓ Denegación de Servicio.
- ✓ Pruebas, escaneos o intentos de obtención de información de un sistema de información.
- ✓ Mal uso de los recursos tecnológicos.

De acuerdo a esa clasificación se enuncian los ejemplos relacionados a los tipos de incidentes clasificados.

- ➢ **Accesos no autorizados:** son ingresos y operaciones no autorizadas a los sistemas, con éxito o no. Forman parte de esta categoría:

  - ✓ Robo de información.
  - ✓ Borrado de información.
  - ✓ Accesos no autorizados exitosos.
  - ✓ Alteración de la información.
  - ✓ Intentos recurrentes y no recurrentes de acceso no autorizado.
  - ✓ Abuso o mal uso de los servicios informáticos (tanto internos como externos) que requieran autenticación.

- ➢ **Código malicioso o malware[30]:** son incidentes que se infiltran en un sistema de información sin autorización del propietario. Son incidentes de código malicioso los siguientes:

[32] **Malware:** Del Inglés Malicious Software, en español Programa Malicioso.

Virus informáticos.

- Troyanos: código malicioso que se introduce en el sistema informático como un programa aparentemente legítimo e inofensivo pero que, al ejecutarlo, permite el acceso remoto del sistema a usuarios no autorizados.

- Gusanos informáticos: código malicioso que, una vez ha accedido al sistema, se va duplicando a sí mismo. No altera los archivos ya instalados pero supone un consumo de recursos importante.

- **Denegación del servicio (DoS[33]):** eventos que producen la pérdida de un servicio en particular, impidiendo su ejecución normal. Suelen ser incidentes de denegación del servicio cuando en el sistema se nota que hay tiempos de respuesta muy bajos y servicios internos y externos inaccesibles sin motivos aparentes.

- **Pruebas, escaneos o intentos de obtención de información de un sistema de información:** son eventos que intentan obtener información sobre las acciones que se producen en un sistema informático. Algunos de estos eventos son:

  - ✓ Sniffers: aplicaciones cuya función es obtener la información que envían los distintos equipos de una red.

  - ✓ Detección de vulnerabilidades: aplicaciones que buscan las vulnerabilidades de un sistema de información para aprovecharse de ello maliciosamente.

[33] **DoS:** Acrónimo del Inglés Denial of Service, en español Denegación de Servicio.

- **Mal uso de los recursos tecnológicos:** eventos que atacan a los recursos tecnológicos de un sistema de información a causa de un mal uso de los mismos. Forman parte de este tipo de eventos:

  - ✓ Violación de la normativa de acceso a internet.
  - ✓ Abuso o mal uso de los servicios informáticos externos o internos.
  - ✓ Abuso o mal uso del correo electrónico.
  - ✓ Violación de las políticas, normas y procedimientos de seguridad informática de una organización.

Toda organización debe tener muy bien identificado sus riesgos y vulnerabilidades. Esto implica que debería además poder gestionar de una forma adecuada los incidentes de seguridad que son parte de los riesgos que toda empresa tiene. El problema de las organizaciones hoy día es que no tienen ni la más remota idea o visibilidad de lo que ocurre con su información y aún no saben ni que tipos de incidentes están ocurriendo en su entorno.

5.3. LOG (Traza de auditoría de eventos)

Según (https://es.wikipedia.org (log), 2018) "En informática, se usa el término log, historial de log o registro a la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos (eventos o acciones) que afectan a un proceso particular (aplicación, actividad de una red informática, etc.). De esta forma constituye una evidencia del comportamiento del sistema. "

Para (Chicano Tejada, 2014, pág. 17) el término "log es un registro oficial de los eventos del sistema producidos a lo largo de un período de tiempo determinado."

Por lo anterior expuesto podemos comprender que un LOG[34] es un registro de los eventos ocurridos en un equipo activo (Servidor, Computador, Switch, Router, UTM[35], IPS[36], etc); practicamente todo equipo activo que posee un sistema operativo para su funcionamiento genera algun tipo de LOG[34]. Por lo general pueden almacenarse ya sea en un archivo de texto, una base de datos o cualquier otro formato que los fabricantes desen emplear en base a algun RFC (Request For Comments, Solicitud de comentarios).

En rasgos generales los logs registran datos de eventos referentes a :

- ✓ Qué tipo de evento ha ocurrido.
- ✓ Quién ha originado el evento.
- ✓ Cuándo se ha producido el evento.
- ✓ Dónde se ha producido el evento.
- ✓ Por qué se ha producido el evento.

En las redes informaticas existen usos de distintos dispositivos conectados y cada dispositivo tiene sistemas operativos con algun tipo de distribuidor o fabricante como los Sistemas Operativos Microsoft Windows, Linux, Unix,

[34] **LOG:** *Registro de seguridad o Traza de auditoría de los eventos*
[35] ***UTM:*** Unified threat management; en español Gestión unificada de amenazas
[36] **IPS:** *Intrusion Prevention System, en español Sistema de Prevención de Intrusos*.

MAC OS[37]. De estos sistemas existen distintas distribuciones y cada uno de ellos genera LOG38. Esto implica que si un usuario desea identificar los distintos eventos que han ocurrido en su equipo debe consultar los LOG[38] del sistemas operativo. Estos LOG[38] almacenan incidentes de seguridad, funcionamientos anomalos, cambios de configuración, instalación de software o dispositvos periferivos, intentos de logeo fallidos, etc.

Tanto Windows como Linux ofrecen la posibilidad de visualizar estos LOG[38]. Cuano visualizamos estos registros podemos detectar y seguir los distintos eventos que han ido sucediendo en el equipo. En el caso de los sistemas operativos Windows de Microsoft se hace uso del visor de sucesos que permite el acceso a los registros del sistema. Los principales registros de eventos son:

- **Registros de aplicación:** almacena eventos registrados por aplicaciones o programas.

- **Registros de seguridad:** registra y almacena eventos ocurridos en los accesos del sistema como los intentos de inicio de sesión (tanto exitosos como fallidos), las introducciones de contraseñas erróneas, bloqueo de cuentas, la utilización de los recursos, etc.

- **Registros de instalación:** registra los eventos que hacen referencia a la instalación de aplicaciones en el equipo. En este registro se puede comprobar si se ha instalado algún código malicioso en el equipo.

- **Registros de eventos reenviados:** eventos que se han reenviado a este registro desde otros equipos.

En el caso de Linux en sus distintas distribuciones almacena los log en formato de texto en distintos archivos. Los principales registros y ubicación de los archivos en Linux son:

- /var/log/auth.log: Eventos de autenticación de usuarios y permisos.

[37]**MAC OS:** Del inglés Macintosh Operating System, en español Sistema Operativo de Macintosh
[38]**LOG***: Registro de seguridad o Traza de auditoría de los eventos*

- /var/log/boot.log: Eventos y servicios empezados cuando se inicia el sistema.
- /var/log/daemon.log: Mensajes sobre permisos o servicios corriendo en el sistema.
- /log/dmesg.log: Mensajes del núcleo Linux.
- /var/log/errors.log: Errores del sistema.
- /var/log/everything.log: Mensajes misceláneos no cubiertos por los otros archivos.
- /var/log/httpd.log: Mensajes y errores de Apache.
- /var/log/mail.log: Mensajes del servidor de correo electrónico.
- /var/log/messages.log: Alertas generales del sistema.
- /var/log/secure: Registro de seguridad.
- /var/log/syslog.log: Registro del sistema de registro.
- /var/log/user.log: Muestra información acerca de los procesos usados por el usuario.

En el caso de dispositivos de comunicación como router, switches y otros como admistradores de ancho de banda o UTM[39] (IPS[40], IDS[41], Anti SPAM[42], Anti Virus) se encargan de enviar sus log a servidores de log llamados syslog y basado en el protocolo syslog. Los mensajes de syslog se suelen enviar vía UDP[43], por el puerto 514, en formato de texto plano. Algunas implementaciones del servidor, como syslog-ng, permiten usar TCP[44] en vez de UDP[43], y también ofrecen Stunnel para que los datos viajen cifrados mediante SSL[45]/TLS[46]. Aunque syslog tiene algunos problemas de seguridad, su sencillez ha hecho que muchos dispositivos lo implementen, tanto para enviar como para recibir. Eso hace posible integrar mensajes de varios tipos de sistemas en un solo repositorio central.

[39] ***UTM:*** Unified threat management; en español Gestión unificada de amenazas.
[40] **IPS:** Intrusion Prevention System, en español Sistema de Prevención de Intrusos.
[41] **IDS:** Intrusion Detection System, en español Sistema de Detección de Intrusos.
[42] **ANTISPAM:** solución de software que permite a los usuarios prevenir o restringir la entrega de spam (correos no deseados)
[43] **UDP:** User Datagram Protocol, en español Protocolo de Datagramas de Usuario.
[44] **TCP:** Transmission Control Protocol, en español Protocolo de Control de Transmisión.
[45] ***SSL:*** *Secure Sockets Layer*; en español capa de puertos seguros)
[46] ***TLS:*** *Transport Layer Security*; en español seguridad de la capa de transporte

5.4. SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT)

Actualmente se han incrementado las medidas de protección de la información y se están administrando una gran cantidad de log generados por los diferentes equipos de la red, servidores y equipos dedicados a la seguridad como IDS[47], IPS[48] o cualquier otro UTM[49] (sistemas de administración unificada de amenazas). Todo lo anterior con propósitos de proteger los diferentes servicios, datos y aplicaciones. Es en este contexto que surge la necesidad de hacer uso de una herramienta capaz de almacenar y gestionar de forma eficiente los diferentes tipos de log y que sea capaz de correlacionar los eventos de tal forma que se puedan no solo visualizar las ocurrencias en tiempo real sino también programar respuestas y alertas acorde a cada evento de seguridad. La respuesta a esta necesidad es la utilización de un SIEM[50] (Security Information and Event Management, en español Información de seguridad y Gestión de eventos).

Según (Secur-IT @C.R.S., 2018) “El término Información de Seguridad y Gestión de Eventos (SIEM), nombrado por Mark Nicolett y Amrit Williams, de Gartner, en 2005, describe las capacidades de los productos de la recopilación, análisis y presentación de información de la red y los dispositivos de seguridad, las aplicaciones de gestión de identidades y accesos, gestión de vulnerabilidades y los instrumentos de política de cumplimiento, sistema operativo, base de datos y registros de aplicaciones. Un punto clave es monitorear y ayudar a controlar los privilegios de usuario y de servicio, servicios de AD y otros cambios de configuración del sistema, así como el abastecimiento de auditoría de registro, revisión, y respuesta a incidentes.”

Según (Sweeny, 2011) de SANS INSTITUTE una solución de Información de Seguridad y Gestión de Eventos (SIEM) es el núcleo de la caja de herramientas de respuesta a incidentes de un trabajador de seguridad de la información. El SIEM[43] comenzó como un producto para recopilar registros de eventos de varios

[47] **IDS:** Intrusion Detection System, en español Sistema de Detección de Intrusos.
[48] **IPS:** Intrusion Prevention System, en español Sistema de Prevención de Intrusos.
[49] ***UTM:*** Unified threat management; en español Gestión unificada de amenazas.
[50] **SIEM:** Security Information and Event Management en español conocido como

sistemas en un servidor central, pero ha crecido para detectar y actuar sobre ciertos tipos de comportamiento y realizar un seguimiento del cumplimiento.

Según (SOFISTIC, 2018) "Los SIEM[51] recopilan aquella información relacionada con la seguridad tanto del hardware de red como de aplicaciones y mediante su correlación o análisis en tiempo real generan diferentes eventos y alertas de seguridad."

La **Figura No.4** Enfoque de SOFISTIC para el SIEM[51] muestra como un SIEM[51] recibe de múltiples fuentes de datos (Hardware o Software) registros de eventos luego correlaciona los eventos para encontrar anomalías identificando ataques y generando alertas.

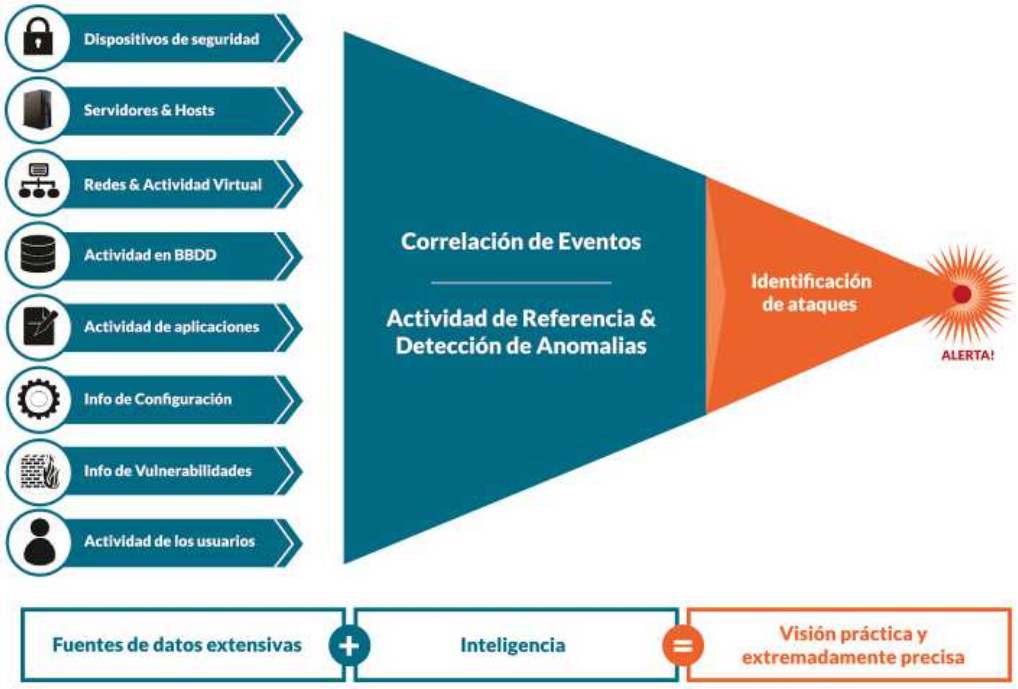


Figura No 4. Enfoque de SOFISTIC para el SIEM (Fuente: SOFISTIC. (05 de septiembre de 2018))

La información de seguridad y gestión de eventos (SIEM) es un enfoque de gestión de la seguridad cuyo objetivo es ofrecer una perspectiva completa de la seguridad de una organización en términos de tecnologías de información. La base central detrás de los sistemas SIEM es la gestión de la seguridad de una

[51]**SIEM:** Security Information and Event Management en español conocido como Sistema de Gestión de Eventos de Seguridad de la Información.

organización desde única ubicación. Los datos relativos a la seguridad de una organización suelen estar distribuidos en varias ubicaciones, por lo que es difícil darse cuenta de las tendencias y patrones anormales. Por esta razón, los productos SIEM[52] y servicios se centran en recopilar todos los datos en un solo lugar y luego analizarlos.

La información de seguridad y gestión de eventos (SIEM) es una pieza de software utilizada en la empresa redes de datos para recopilar registros de entrada y alertas de una variedad de sistemas de seguridad tales como Firewalls, Enrutadores y servidores e intentan interpretar los eventos recopilados, así como informar a los operadores de seguridad de ocurrencias inusuales (Miller et al, 2010). SIEM[52] es una idea relativamente nueva, pionera en hace una década y aún evoluciona rápidamente aún. Más importante aún, ahora se ha convertido en una poderosa herramienta de seguridad que obtiene información de muchos sistemas a nivel de red y de aplicación, teniendo una percepción de los eventos de seguridad y la capacidad de acceder a las bases de datos de vulnerabilidad, por ejemplo, sistema conocido debilidades y su explotación. SIEM[52] también puede tener una herramienta de informe para ayudar a los analistas de seguridad con una investigación de eventos y una producción de informes.

Las soluciones SIEM[52] son una combinación de las categorías de productos formalmente dispares SIM[53] (Security Information Management) and SEM[54] (Security Event Manager). La tecnología SIEM[52] proporciona un análisis en tiempo real de las alertas de seguridad generadas por el hardware y software de red. Las soluciones SIEM[52] pueden venir como software, appliance[55], o administración de servicios, y también son utilizados para registrar datos de seguridad y generar reportes para fines de complimiento.

[52]**SIEM:** Security Information and Event Management en español conocido como Sistema de Gestión de Eventos de Seguridad de la Información.
[53]***SIM:*** Security Information Management, en español Gestión de Información de Seguridad
[54]***SEM:*** *Security Event Management, en español Gestión de Eventos de Seguridad.*
[55]**Appliance:** Dispositivo con una función específica y configuración limitada para el usuario

5.4.1. CAPACIDADES DE UN SIEM

Algunas de las capacidades de un SIEM son:

- **Colección de datos:** En un caso de uso típico, una solución SIEM[56] debe ser capaz de gestionar registros de incidentes de cualquier elemento de la infraestructura tecnológica, tales como: firewalls, servidores proxy, bases de datos, detección y prevención de intrusiones, sistemas operativos (OS[57]), enrutadores, Switch, sistemas de control de acceso, etc. Algunos de estos pueden compartir funciones de registro y alertas similares, pero con frecuencia, hay una variación significativa en el formato, el protocolo y la información proporcionada. La recolección de datos ocurre en un número de maneras, a menudo depende de la solución y el sistema final. Algunos sistemas pueden ser capaces de conectarse directamente con el SIEM[56], utilizando un protocolo estándar, mientras que otros pueden utilizar un protocolo o una API[58], que requiere que la solución SIEM[56] entienda el protocolo / API[58] o que se añada una aplicación de tercero, otros sistemas finales simplemente escriben un archivo de registro de texto plano que el SIEM[56] o un agente recuperará periódicamente.

- **Agregación de datos:** Una vez que la solución SIEM[56] recopila la información de sus diversas fuentes, esta combina los datos en un solo almacén de datos, facilitando la correlación junto con otras funciones de EM[59], las funciones forenses y de presentación de informes de SIM[60]. La agregación puede parecer sencilla, pero presenta una serie de retos y consideraciones, la arquitectura debe ser considerada también, dependiendo del tamaño y la huella física de una empresa, la cantidad de datos que se recoge, y la infraestructura de TI[61], la acumulación puede hacerse de forma centralizada o en sistemas distribuidos.

[56] **SIEM:** Security Information and Event Management en español conocido como Sistema de Gestión de Eventos de Seguridad de la Información.
[57] **OS:** Acrónimo de Operative Sistem, en español Sistema Operativo.
[58] **API:** Acrónimo de Application Programming Interface, en español Interfaz de programación de Aplicaciones.
[59] **EM:** Event Management en español Gestión de Eventos
[60] ***SIM:*** Security *Information Management, en español Gestión de Información de Seguridad*
[61] **TI:** Tecnologías de la Información.

- **Correlación de eventos:** Es la función de vincular múltiples eventos de seguridad o alertas, por lo general dentro de un mismo tiempo y a través de múltiples sistemas, para identificar la actividad anómala que no sería evidente en un evento individual. Para lograr esto, la solución SIEM[62] debe tener reglas que le indica al motor de correlación sobre los tipos de eventos que debe tratar de correlacionar y las condiciones que justifican una alerta. La mayoría de las soluciones han preestablecido los conjuntos de normas, pero con frecuencia se requiere el ajuste de estas normas preexistentes, como es la creación de reglas personalizadas adaptadas al entorno.

- **Normalización de datos:** La normalización es el proceso de resolución de diferentes representaciones de los mismos tipos de datos en un formato similar, en una base de datos común. Las soluciones SIEM[62] extraen información de un gran número de dispositivos y mientras estos dispositivos suelen recopilar la misma información (por ejemplo, la fuente y la dirección de red de destino, tipo de protocolo, el tiempo, fecha) esto es reportado a menudo en diferentes formatos. El proceso de normalización extrae información común y la expresa en un formato coherente, lo que permite una comparación directa de diferentes eventos. Por ejemplo, una vez normalizado, un evento registrado de un UTM[63] Sophos tendrá el mismo aspecto como uno de un firewall de Check Point ® y cualquier información propietaria se habrá desechado.

- **Alerta:** el análisis automatizado de eventos correlacionados y la producción de alertas, para notificar a los destinatarios de los problemas inmediatamente. Una alerta puede ser un tablero de instrumentos, o enviarse a través de canales de terceros, tales como el correo electrónico. Esta Funcionalidad está disponible con la solución, ya que es importante para la rápida atención frente a eventos de seguridad.

[62]**SIEM:** Security Information and Event Management en español conocido como Sistema de Gestión de Eventos de Seguridad de la Información.
[63]***UTM:*** Unified threat management; en español Gestión unificada de amenazas.

- **Reportes:** La función de informes es a menudo el foco central del cumplimiento (compliance). Es fundamental para el SIEM[64] para que los procesos de definición, la generación y exportación de informes que sea tan versátil y fácil de usar como sea posible. Los informes personalizados y plantillas de informes serán soportados por la solución implementada, permitiendo diferentes tipos de reportes según la política de cumplimiento.
- **Forense:** La capacidad de buscar datos de registro y alertas para los indicadores de las actividades maliciosas o de otras actividades anómala es la función forense del SIEM[64]. La función forense que es apoyada por los procesos de correlación de eventos y de normalización, requiere capacidades de consulta altamente personalizables y detalladas y acceso a los archivos de registro bruto u originales y datos históricos. Trabajando en conjunto, estas tecnologías pueden mejorar en gran medida las capacidades de investigación de los analistas de seguridad, así como la recopilación de datos, tecnologías de agregación y correlación, mejoran su capacidad para detectar y responder a eventos en tiempo real.

- **Dashboards**[65]**:** Se proporcionan paneles para resumir los datos y obtener una instantánea rápida de la postura de seguridad. Están destinados a ser un punto de partida para un análisis más profundo. La amplia gama de vistas y las representaciones de datos ayuda a ver patrones o identificar una actividad que no está siguiendo un patrón estándar.

- **Cumplimiento:** Las aplicaciones SIEM[64] se pueden emplear para automatizar la recopilación de datos y la elaboración de informes que se adapten a los procesos existentes de seguridad, gobernabilidad y auditoría.

[64]**SIEM:** Security Information and Event Management en español conocido como Sistema de Gestión de Eventos de Seguridad de la Información.
[65]**Dashboards:** En español Tablero. En contexto del SIEM Tablero de controles.

- **Retención:** SIEM[66] / SIM[67] emplea soluciones a largo plazo de almacenamiento de datos para facilitar la correlación de datos con el tiempo, y para proporcionar la retención necesaria para los requisitos de cumplimiento. Un largo plazo de retención de registros de datos es crítica en la investigación forense, ya que es poco probable que el descubrimiento de una violación de la red sea en el momento de la infracción se produzcan.

[66] **SIEM:** Security Information and Event Management en español conocido como Sistema de Gestión de Eventos de Seguridad de la Información.
[67] ***SIM:*** Security Information Management, en español Gestión de Información de Seguridad

5.4.2. ESTRUCTURA DE UN SIEM

Un sistema SIEM[68] consta de una serie de elementos operativos, con cada elemento a cargo de una tarea particular. Para que todo el sistema funcione con precisión, todos los elementos tienen que ser correctos y trabajar juntos. Existen muchas versiones de un sistema SIEM[68], teniendo cada sistema elementos suplementarios, pero esta sección describirá un sistema SIEM[68] básico.

Como se ilustra en la **Figura No.5** Estructura de un SIEM[68]; una solución SIEM68 básica consta de seis elementos independientes, y estos elementos son: el dispositivo de origen, la recopilación de registros, el análisis o la normalización de registros, el motor de reglas o motor de correlación, almacenamiento de registro y monitoreo de eventos. Como se indica en (Miller et. al, 2010,pág. 78), cada elemento puede funcionar independientemente, pero un sistema SIEM[68] no funcionará correctamente sin todos los elementos trabajando juntos.

Figura No.6 Estructura de un SIEM

Figura No 5. Estructura de un SIEM (adaptada de Miller et al, 2010,pág.78).

DISPOSITIVO DE ORIGEN

El **dispositivo fuente** es el primer elemento de la estructura SIEM[68] y sirve como entrada para el sistema SIEM[68]. De acuerdo con (Miller et. al, 2010, pág. 78), cualquier tipo de dispositivo o aplicación puede ser un dispositivo fuente, siempre y cuando los registros se puedan recuperar de él, y luego el sistema SIEM pueda almacenar y procesar. Por lo tanto, un dispositivo fuente no

[68]**SIEM:** Security Information and Event Management en español conocido como Sistema de Gestión de Eventos de Seguridad de la Información.

es realmente un segmento del sistema SIEM[69] que se compra como parte del sistema SIEM[69], sino que es esencial para los fines de la organización.

Un sistema SIEM[69] no puede funcionar sin los registros y otra información generada por el dispositivo fuente de acuerdo con (Miller et. al, 2010, pág. 78). Por lo tanto, es muy importante analizar en cada organización en orden para decidir qué dispositivo es crítico para la recuperación de sus registros.

RECOPILACIÓN DE REGISTROS

Después de seleccionar los dispositivos fuente, es **esencial recuperar los registros** de esos dispositivos y transferirlos al sistema SIEM[69]. Esta operación se llama recopilación de registros, y dos técnicas esenciales para la recopilación de registros son los métodos de empujar (**push**) y extraer (**pull**). El método push se utiliza cuando un dispositivo fuente envía sus registros al sistema; mientras que en el método de extracción, el sistema recupera los registros de los dispositivos fuente. (Miller et. al, 2010, pág. 82) dicen que la ventaja de usar un método push es que simplifica la instalación y configuración del sistema SIEM[69]. En la mayoría de los casos, solo se necesita instalar un receptor y el dispositivo de origen debe enviar sus datos de registro a este receptor. Un ejemplo de un método push es el protocolo syslog, donde un dispositivo fuente necesita configurarse con la dirección IP o el nombre DNS[70] de un servidor syslog en su red. Este dispositivo de origen enviará entradas de registro al receptor syslog, que en realidad es parte del sistema SIEM69. Sin embargo, una desventaja de usar un método push es que puede presentar algunos problemas de seguridad. Un ejemplo de un problema de seguridad de este tipo ocurre cuando se usa el protocolo syslog sobre el protocolo UDP[71]. Porque el protocolo UDP[71] no es orientado a conexión, no se garantiza que los paquetes que contengan los registros lleguen al servidor de destino. En contraste, una desventaja de usar un método de extracción (pull) según (Miller et. al, 2010, pág. 82) es que los registros pudrían no llegar al sistema SIEM[69] en tiempo real.

[69]**SIEM:** Security Information and Event Management en español conocido como Sistema de Gestión de Eventos de Seguridad de la Información
[70]**DNS:** *Domain Name System, en español Sistema de nombre de dominio*
[71]**UDP**: *Datagram Protocol o, en español Protocolo de datagrama de usuario.*

NORMALIZACIÓN DE REGISTROS

El siguiente elemento de la estructura SIEM[72] es la **normalización**, que trata sobre la conversión de registros a un único formato estandarizado. Las salidas del elemento anterior, la recopilación de registros, eran registros que están en su formato original, pero estos registros no son útiles para un sistema SIEM[72] y, por lo tanto, deben ser normalizados. La **Figura No.6** Registro de Windows muestra una entrada del registro de eventos de Windows y la Figura 7 muestra un mensaje de syslog de Cisco ASA, ambos ejemplos de un evento de un usuario que inicia sesión en un sistema. Sin embargo, es obvio a partir de estas cifras que diferentes proveedores utilizan diferentes formatos para representar sus registros. Por lo tanto, para comprender los eventos, es necesario convertirlos a un formato común. La **Figura No 8** ilustra ambos registros (**Figura No.6** y **Figura No.7**) después del procedimiento de normalización. La normalización no solo es útil para mejorar la legibilidad de los eventos, sino también para habilitar un formato de regla estandarizado según (Miller et. al, 2010. Pág. 86).

[72]**SIEM:** Security Information and Event Management en español conocido como Sistema de Gestión de Eventos de Seguridad de la Información.

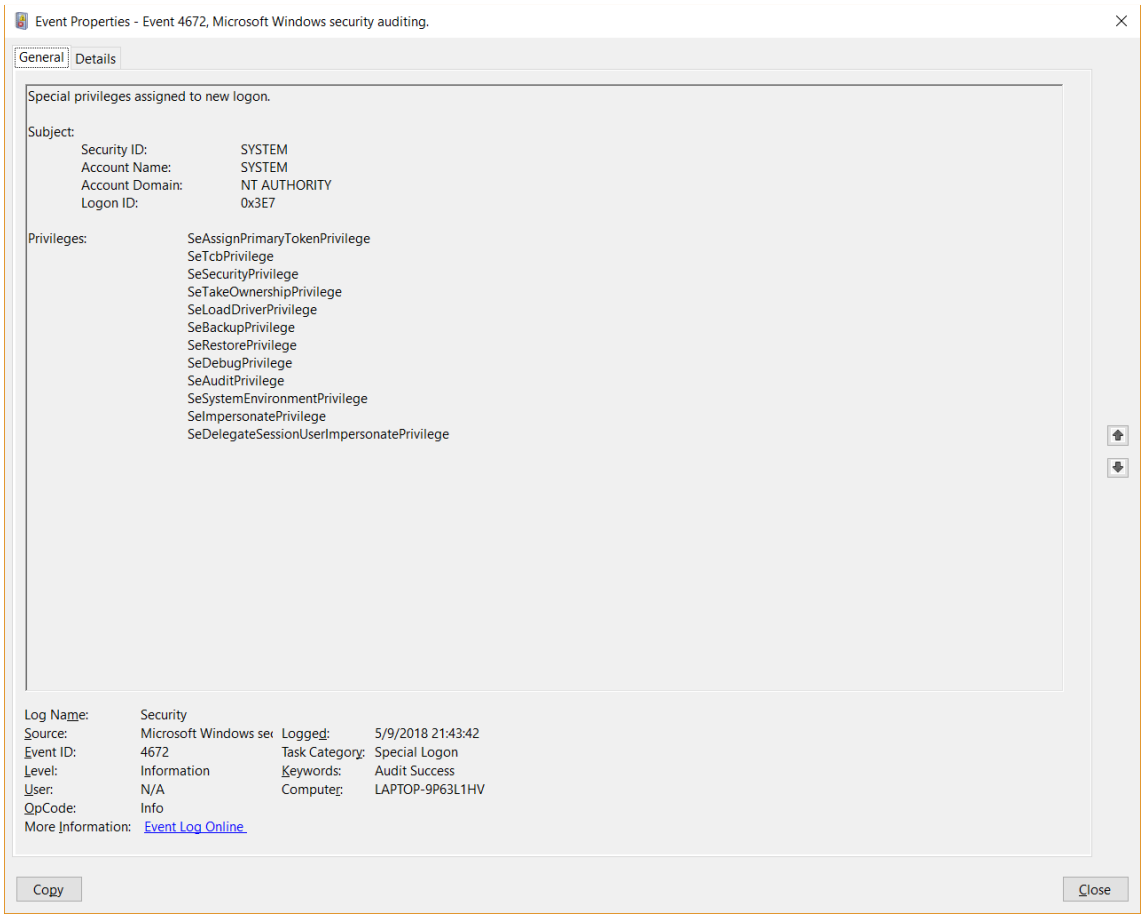


Figura No 6. Registro de Windows (Fuente: PC Personal, 2019, Registro de Seguridad)

Priority	Hostname	Message
Local4.Info	192.168.1.1	:%ASA-sys-6-605005: Login permitted from 192.168.1.18/42925 to INSIDE:192.168.1.1/

Figura No 7. Mensage Syslog de un Cisco ASA
(adaptada de Miller et al, 2010,pág. 85, Figure 5-2 Cisco ASA syslog message).

Time	Date	Source Device IP Address	Event Message	Event
22:54:53	CST 09-Sep-18	192.168.1.1	User login	ASAsys-6-605005
22:54:53	CST 09-Sep-18	192.168.1.18	User login	Security: 680

Figura No 8. Evento Normalizado
(adaptada de Miller et al, 2010,pág. 86, Table 5-1 Correlated Event).

MOTOR DE REGLAS/ MOTOR DE CORRELACIÓN

Un **motor de reglas** se usa para activar alertas basadas en ciertas condiciones que ocurren en los registros normalizados. La lógica booleana se usa generalmente para escribir las reglas y decidir si se han encontrado condiciones particulares según (Miller et. al, 2010, pág. 86). La **Figura No.9** Reglas de Acceso de Administrador muestra las reglas de inicio de sesión de administración donde se genera una alerta se activa cuando un administrador local inicia sesión en un servidor. De esta forma el SIEM[73] en lugar de tener varias reglas activadas para los diferentes tipos de inicios de sesión de administrador (Ej. Admin, Administador, Administrator, root, etc.), puede escribir una sola regla utilizando la lógica interna de SIEM para activar una regla basada en variables múltiples.

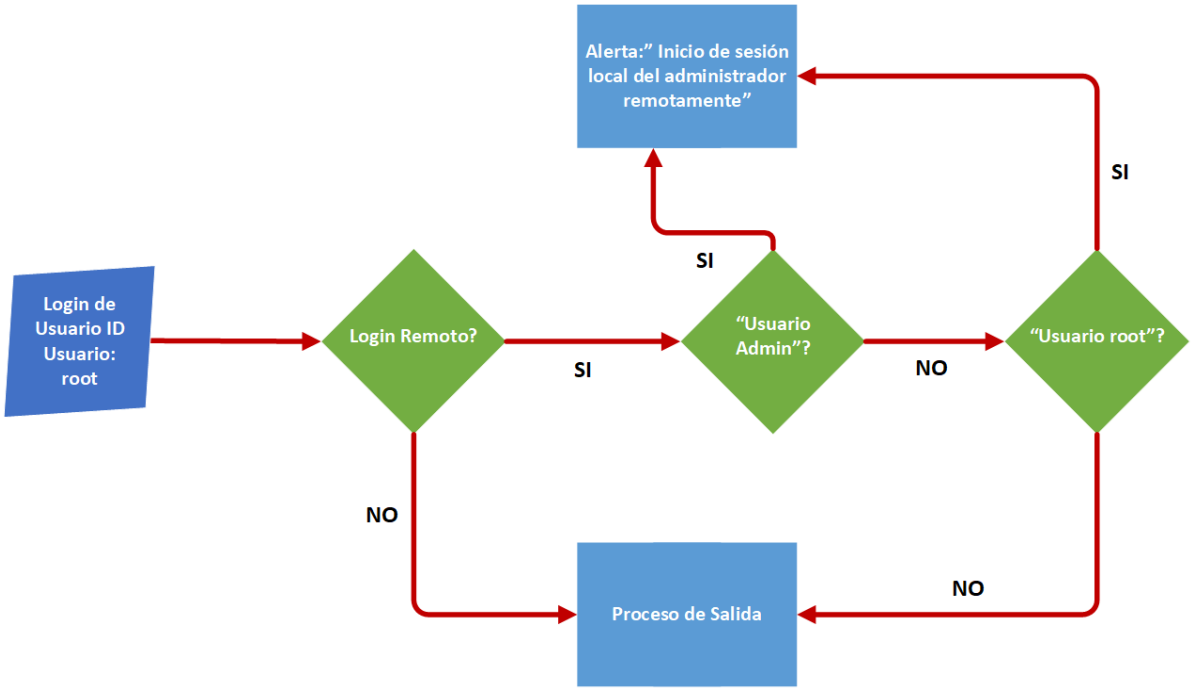


Figura No 9. Reglas de Acceso de Administrador
(adaptada de Miller et al, 2010,p.87, Figure 5-3 Administrator login rules).

[73]**SIEM:** Security Information and Event Management en español conocido como Sistema de Gestión de Eventos de Seguridad de la Información

Un subconjunto de un motor de reglas es responsable de hacer coincidir varios eventos en un evento correlacionado, por lo tanto, este subsistema se conoce **como motor de correlación**. La correlación se realiza para simplificar los procedimientos de respuesta a incidentes. Por lo tanto, solo uno evento se desencadena cuando llegan varios eventos relacionados desde varios dispositivos de origen. De tal forma que si un dispositivo intenta generar un ataque de fuerza bruta se puede crear una regla que alerte y correlacione todos los orígenes y destinos detectando un patrón anómalo que genere alerta cuando más de cuatro destinos están fallando el inicio de sesión desde un mismo origen. La **Figura No.10 Ejemplo de Evento Correlacionado** muestra cómo trabaja el motor de correlación.

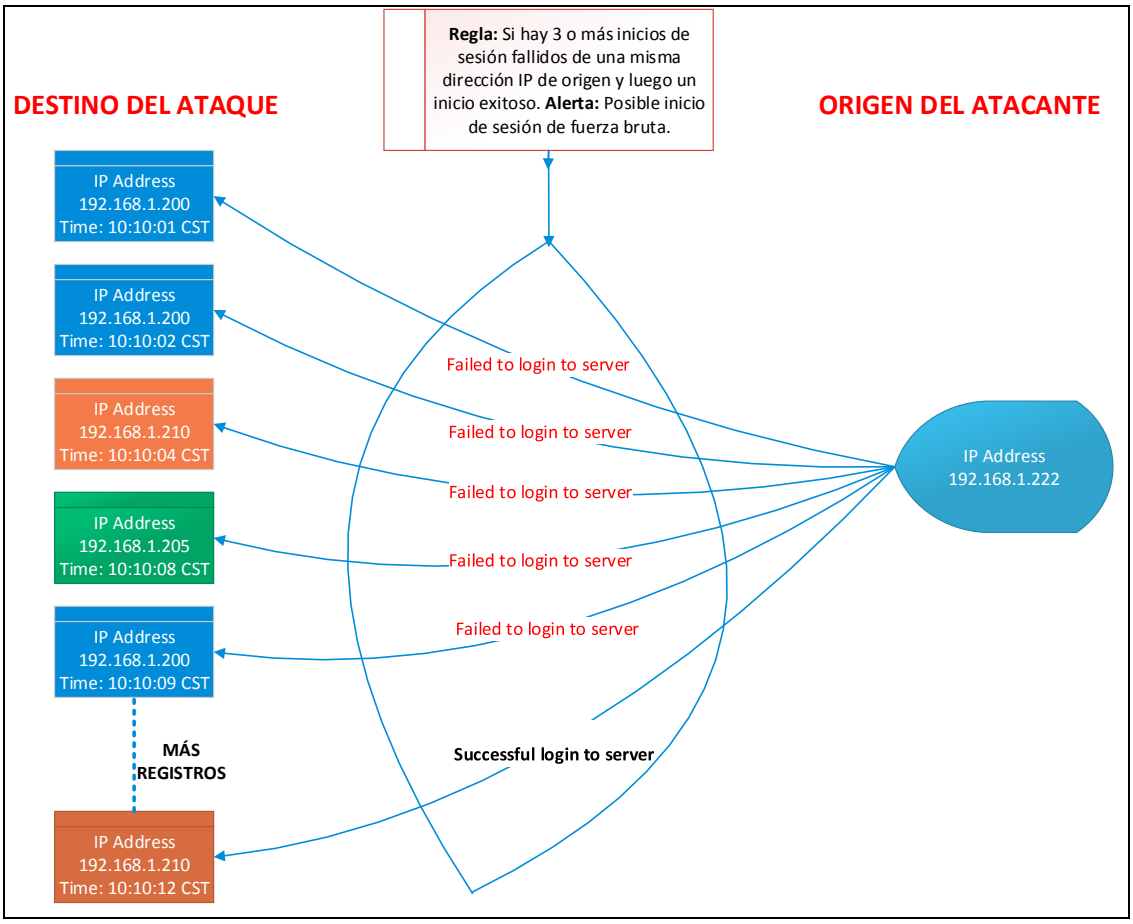


Figura No 10. Ejemplo de Evento Correlacionado(adaptada de Miller et al, 2010,p.89, Figure 5-4 Correlated Event Example).

En un SIEM[74] ya funcionando se podría crear una regla correlacionada que emplee un pseudocódigo como el siguiente:

> **If** [(failed logins >= 3) and then (Successful Login)] from the same source within 20 seconds = Possible Brute Force Compromise

El pseudocódigo descrito anteriormente corresponde al ejemplo de evento correlacionado en la **Figura No.10**; ejemplo en el cual se observa con claridad que un solo origen está intentando efectuar inicios de sesión a múltiples destinos y que al final consigue iniciar sesión en un equipo activando la regla de correlación que establece que si existen más de tres intentos fallidos y luego hay uno exitoso en un rango de 20 segundos se puede estar enfrentando un posible ataque de fuerza bruta.

ALMACENAMIENTO DE REGISTROS

El almacenamiento de registro se utiliza para acumular numerosos registros que llegan al sistema SIEM[74]. Estos registros tienen que ser almacenado por razones de retención y consultas históricas. Tres métodos de almacenamiento de registro son típicamente utilizados, y esos son: almacenamiento de bases de datos, almacenamiento de archivos de texto plano y almacenamiento de archivos binarios. El almacenamiento de base de datos es el método más común de almacenar registros debido a los métodos simples para interacción y recuperación de datos.

Plataformas de bases de datos típicas, como Oracle, MySQL, Microsoft SQL, etc., se utilizan para almacenar los datos. El almacenamiento de archivos de texto plano utiliza archivos de texto para almacenar los datos en un dispositivo en formato legible. Sin embargo, este método no se utiliza con frecuencia debido a su bajo rendimiento y escalado pobre. El formato de archivo binario almacena datos binarios, pero solo lo utilizan ciertos sistemas SIEM[74].

[74] **SIEM:** Security Information and Event Management en español conocido como Sistema de Gestión de Eventos de Seguridad de la Información

MONITOREO DE EVENTOS

El monitoreo de eventos es el último elemento de una solución básica de SIEM[75]. Esta etapa se usa para la explotación de los registros que se almacenaron en un sistema SIEM[75] en la etapa anterior. El propósito del monitoreo de eventos es utilizar los datos almacenados y beneficiarse de ellos. Se proporciona una interfaz para la supervisión de eventos que proporciona una descripción general de todo el entorno.

Un SIEM[75] tendrá una consola de interfaz que estará basada en la web o en la aplicación y se podrá cargar en una estación de trabajo. Ambas interfaces le permitirán interactuar con los datos almacenados en su SIEM[75]. La consola ya sea basada en la web o en la aplicación se utilizará para administrar el SIEM[75]. Con la interfaz de la aplicación SIEM[75] se permitirá a sus manejadores de incidentes o ingenieros de sistemas una vista única de su entorno de infraestructura de red que normalmente antes del SIEM[75] tendrían que ir a los diferentes dispositivos y ver los registros en sus formatos nativos. El SIEM[75] facilita la visualización y el análisis de todos estos registros diferentes porque el SIEM[75] normaliza los datos. Dentro de la consola de administración y monitoreo de SIEM[75] se podrá desarrollar el contenido y las reglas que se utilizarán para extraer la información de los eventos que se procesan.

[75]**SIEM:** Security Information and Event Management en español conocido como Sistema de Gestión de Eventos de Seguridad de la Información

5.4.3. BENEFICIOS DE UN SIEM

Los beneficios que se obtienen cuando una organización realiza una implementación propia de la solución son:

- Mayor valor de la inversión en seguridad de la tecnología-SIEM[76] permite un uso más eficaz del registro de seguridad e información de eventos, lo que permite al equipo de seguridad darse cuenta de todo el potencial de los sistemas de seguridad.

- Reportes eficientes: Desarrollo y entrega de informes completos y eficientes a la gerencia de TI[77], esto puede ser casi un trabajo a tiempo completo para un administrador de seguridad. Mediante el soporte a una amplia gama de sistemas y facilitar la mayor parte del proceso de recopilación y notificación de registro a través de herramientas automatizadas y plantillas de informes, una solución SIEM[76], puede reducir una tarea que antes llevaba días a una cuestión de horas, liberando al administrador de seguridad para centrarse mejor en prioridades y responsabilidades.

- Reducción de capital y costos operacionales: Herramientas convergentes tales como SEM[78], SIM[79], sistemas de análisis y administración de registros y sistemas de monitoreo de actividad en bases de datos, todo en una misma solución, permitiendo a la compañía ahorrar en tiempo y dinero. Los costos de compra y mantenimiento asociados con muchos sistemas de monitoreo y análisis pueden ser reducidos teniendo una única solución SIEM[76].

[76] **SIEM:** Security Information and Event Management en español conocido como Sistema de Gestión de Eventos de Seguridad de la Información
[77] **TI:** *Tecnologías de la Información*
[78] ***SEM:*** *Security Event Management, en español Gestión de Eventos de Seguridad.*
[79] ***SIM:*** Security Information Management, en español Gestión de Información de Seguridad

- Reducción del riesgo de incumplimiento de los sistemas – SIEM[80] proporcionara a la empresa informes detallados. Durante una auditoría o investigación, la empresa tendrá la información necesaria para demostrar el cumplimiento o la debida diligencia.
- Amplio apoyo de la organización para obtener información - Un sistema de seguridad SIEM[80] eficaz implica una amplia base de actores que deben trabajar juntos, con frecuencia en equipos multi-funcionales, para evaluar los eventos, crear informes y tomar acciones para abordar los incidentes señalados por el sistema SIEM[80].

- Detección temprana de incidentes de seguridad - una adecuada solución SIEM[80] proporciona a los analistas de seguridad un conjunto de herramientas que pueden mejorar en gran medida su eficacia. Un equipo de seguridad más eficaz tiene una mayor probabilidad de interceptar y abordar los eventos de seguridad en sus primeras etapas antes de que puedan afectar significativamente a la empresa.

- Los SIEM[80] pueden ser implementados en empresas u organización con o sin un sistema de gestión de seguridad de la información (SGSI[81]). En nuestro caso la EAAI[82] no está apegada a un estándar como el ISO83 27001; sin embargo esto no es un impedimento para la implementación de un SIEM[80] si se cuenta con los siguientes elementos: Caracterización de activos que se van a monitorear, Análisis de vulnerabilidad sobre los activos y su nivel de riesgos, plan de contingencias.

[80]**SIEM:** Security Information and Event Management, en español conocido como Sistema de Gestión de Eventos de Seguridad de la Información.
[81]**SGSI:** *Sistema de Gestión de Seguridad de la Información*
[82]**EAAI:** *Empresa Administrador de Aeropuertos Internacionales.*
[83]**ISO:** International Organization for Standardization, en español Organización Internacional de Normalización/estandarización.

5.4.4. VENTAJAS DE IMPLEMENTAR UN SOFTWARE SIEM

Implementar un SIEM[84] brindará a cualquier empresa las bases para desarrollar su propio **NOC** (Network Operation Center, Centro de Operaciones de Redes) o un **SOC** (Security Operation Center, Centro de Operaciones de seguridad). Ya que se poseerá información almacenada de log de equipos de seguridad, correlación de eventos y alertas resultando más fácil detectar tendencias y centrarse en patrones fuera de lo común.

Cuando un SIEM[84] está operando se espera que brinde ventajas al tener menores tiempos de respuestas en el reconocimiento de atacantes, generación de alertas y almacenamiento de eventos de seguridad que podrán utilizarse para investigaciones.

Algunas ventajas de implementar un SIEM[84] son:

- **Detección de amenazas desconocidas:** Para detectar amenazas utiliza machine learning (en español aprendizaje automatizado o aprendizaje de maquinas, rama de la inteligencia artificial) y tecnologías de última generación que permiten detectar anomalías en los comportamientos. Todo esto sin necesidad de disponer de reglas o firmas. La ventaja es que el SIEM[84] alerta sobre la actividad potencialmente malintencionada.

- **Mayor velocidad en la investigación de las alertas:** El contexto agregado, la visibilidad y la inteligencia de amenazas proveen a los analistas de seguridad un mayor conocimiento en la toma de decisiones acerca del modo más oportuno de actuar. Esta ágil respuesta proviene de la contextualización y la recopilación de la inteligencia de amenaza relacionada con la alerta.

[84] **SIEM:** Security Information and Event Management, en español conocido como Sistema de Gestión de Eventos de Seguridad de la Información.

- **Búsqueda de amenazas en registros archivados:** La capacidad de almacenar los registros de seguridad posibilita la búsqueda de algunos de los ataques más difíciles de detectar como los que permanecen inactivos durante largos periodos de tiempo dentro de la red interna. SIEM[85] facilita la detección de amenazas al emplear herramientas analíticas para la búsqueda en registros archivados.

- **Monitoreo de las actividades de la red**: Las soluciones de SIEM[85] proveen de la información necesaria sobre la actividad de los usuarios y los dispositivos empleados para cada interacción identificando signos de comportamiento malicioso, como cuentas comprometidas o endpoints (equipos finales) infectados.

[85]**SIEM:** Security Information and Event Management, en español conocido como Sistema de Gestión de Eventos de Seguridad de la Información.

5.4.5. DESCRIPCIÓN DEL MERCADO DEL SIEM

Según (Kelly Kavanagh, 2018) “El mercado de información de seguridad y gestión de eventos (SIEM) se define por la necesidad del cliente de analizar datos de eventos en tiempo real para la detección temprana de ataques dirigidos y violaciones de datos, y recolectar, almacenar, analizar, investigar e informar datos de eventos para incidentes respuesta, forense y cumplimiento regulatorio. Los proveedores incluidos en nuestro análisis Magic Quadrant tienen productos diseñados para este propósito, y comercializan y venden activamente estas tecnologías al centro de compras de seguridad.”

Según Kelly Kavanagh de Gartner en su informe nos indican que las herramientas SIEM[86] unifican los datos de eventos generados por dispositivos de seguridad ya sean de la infraestructura de red, sistemas o aplicaciones. En todo la funcionalidad el SIEM[86] la fuente principal de datos son los datos de registro de cada sensor o equipo activo; los SIEM[86] también pueden procesar otras formas de datos como NetFlow y paquetes de red, o información contextual sobre usuarios, activos, amenazas y vulnerabilidades que se pueden encontrar dentro o fuera de la empresa y que pueden ser útil para enriquecer registros y datos sin procesar.

Como parte del funcionamiento del SIEM[86] se deben de normalizar los registros que se reciben de distintas fuentes para que puedan correlacionarse y analizarse con fines específicos como administración de amenazas, monitoreo de eventos de seguridad de red (SEM[87]), monitoreo de la actividad del usuario e informes de cumplimiento.

Figura No.11. Cuadrante mágico para información de seguridad y gestión de eventos (SIEM[86]). Fuente: Gartner (diciembre de 2017); nos muestra los principales software SIEM[86] existentes en el mercado.

[86] **SIEM:** Security Information and Event Management, en español conocido como Sistema de Gestión de Eventos de Seguridad de la Información.
[87] ***SIM:*** Security *Information Management, en español Gestión de Información de Seguridad*

.

Figura No 11. Cuadrante mágico para información de seguridad y gestión de eventos (SIEM).

Como se puede observar existen productos muy bien posicionados en el mercado siendo los líderes como: Splunk, IBM, LogRhythm, McAffe.

También se pueden observar otras categorías como Retadores, Visionarios y jugadores de nicho como: SolarWinds, Allien Vault, Fortinet, EventTracker, etc.

6. DISEÑO METODOLÓGICO

6.1. TIPO DE INVESTIGACIÓN

El tipo de investigación a desarrollar estará basada en un diseño de investigación descriptiva. De tal forma todo el desarrollo de la tesis será con objetivo de demostrar que el nivel de visibilidad y tiempo de respuesta será más eficiente para la EAAI[88] al tener un SIEM[89] implementado.

[88] **EAAI:** *Empresa Administradora de Aeropuertos Internacionales*
[89] **SIEM:** Security Information and Event Management, en español conocido como Sistema de Gestión de Eventos de Seguridad de la Información.

6.2. METODOLOGÍA DE INVESTIGACIÓN

Para este efecto se estarán investigando y probando las diferentes alternativas de SIEM[90] disponibles y de acuerdo a las características ofertadas y la disponibilidad del software se realizará la elección del Software SIEM[90] a implementar. Como líneas principales a seguir esta documentar todo lo referente a los SIEM[90], luego se procederá a elegir un SIEM[90] a implementar.

Como parte de las tareas a realizar de forma implícita serán:

- ✓ Establecer políticas de tráfico de la red que permitan tener activos solo los puertos y servicios que se utilizan brindando un marco de referencia para los procedimientos a implementar bajo cada política.
- ✓ Centralizar los log de dispositivos de red y servidores en una sola consola que genere alertas y brinde monitoreo vía correo electrónico, mensajes de red o SMS[91] de cualquier ataque que se esté perpetrando al perímetro WAN[92] o a la LAN[93].
- ✓ Documentar la gestión de los incidentes y alarmas vía sistema de tickets en base a los procedimientos de gestión de incidentes.
- ✓ Crear el perfil y lineamientos de un equipo de monitoreo y respuesta a incidentes 24x7x365.
- ✓ Implementar herramientas de software libre para monitoreo de red, monitoreo de vulnerabilidades, administración de log y gestión de alertas.
- ✓ Establecer perfil de oficial de seguridad.
- ✓ Establecer perfil de personal de investigación y desarrollo de infraestructuras de redes.

[90] **SIEM:** Security Information and Event Management, en español conocido como Sistema de Gestión de Eventos de Seguridad de la Información.
[91] **SMS:** Short Message Service, en español Servicio de Mensajes Cortos.
[92] **LAN:** Local Area Network, en español Red de Área Local.
[93] **WAN:** Wide Area Network, en español Red de Área Amplia.

El software SIEM[94] elegido deberá ser compatible con la infraestructura tecnológica de la EAAI[95]. Durante el proceso de implementación se podrá hacer uso de software libre que funcione como IDS[96] o IPS[97] para efectos de tener más fuentes generadoras de eventos o sucesos de seguridad.

El proceso metodológico a realizar es:

- Investigación de distintos tipos de software SIEM[94] disponibles y que estén bien posicionados en el cuadrantes Mágico de Gartner.
- Se procederá a probar distintos software disponibles y se analizará cual es más viable para la organización.
- Se seleccionarán dos software para pruebas y se tomarán como pautas las funcionalidades y los costos de implementación.
- Se presentará proyecto a la Gerencia de TI[98] para solicitar autorización e iniciar los estudios.
- Se establecerá un plan de actividades de acuerdo al cronograma de trabajo del proyecto de tesis.
- El software seleccionado se procederá a documentar todo lo referente a su arquitectura, funcionalidades y características.
- Se valorarán todos los requisitos necesarios para implementar el SIEM[94].
- Se seleccionarán los sensores que se integrarán al SIEM[94]
- Se llevará a cabo la instalación y configuración del SIEM[94].
- Se integrará al SIEM[94] todos los sensores que se eligieron.
- Se procederá a realizar pruebas y ajustes al SIEM[94].
- Durante todas las etapas se documentará el proceso.

[94]**SIEM:** Security Information and Event Management, en español conocido como Sistema de Gestión de Eventos de Seguridad de la Información.
[95]**EAAI:** *Empresa Administradora de Aeropuertos Internacionales.*
[96]**IDS:** Intrusion Detection System, en español Sistema de Detección de Intrusos.
[97]**IPS:** Intrusion Prevention System, en español Sistema de Prevención de Intrusos.
[98]**TI:** *Tecnologías de la Información.*

6.3. OBTENCIÓN DE INFORMACIÓN

La información de la empresa referente a la topología de red, equipos activos, configuraciones y todos los requisitos necesarios para implementar el SIEM[99] serán canalizados por medio de la autorización del Gerente de TI[100] al Implementador del SIEM[99], Jefe de Infraestructura de Red y Administración de base de datos, que es parte integral de la empresa y que cuenta con toda la información necesaria de la empresa para valorar en las etapas requeridas de la implementación del SIEM[99].

[99] **SIEM:** Security Information and Event Management, en español conocido como Sistema de Gestión de Eventos de Seguridad de la Información.
[100] **TI:** *Tecnologías de la Información.*

7. REQUISITOS DE DISEÑO DEL SIEM

7.1. REQUERIMIENTOS PARA IMPLEMENTACIÓN DE SIEM

Evaluación de Riesgos

Identificación de activos de la organización

Para realizar la evaluación de riesgos la primera tarea fue identificar los activos claves de la organización que soportan todos los procesos y servicios informáticos de la empresa, además en la **Tabla 1. Costos de activos de la EAAI**[101] podemos ver los costos de cada uno de los activos.

Tabla 1. Costos de activos de la EAAI.

Activos Informáticos	Cantidad	Costo Aproximado
Servidores (2 Procesadores Intel Xeon 2.4 Ghz - 3.2 Ghz, Ram 16G-32GB), Discos Duros 4-6 (300 GB), Controladora Raid, Tarjeta de Acceso Remoto Enterprise, Fuentes Redundantes 530-730 Watts)	12	U$ 96,000
Switches Administrables 24 Puertos (24 Puertos 10/100/1000, 4x SFP) Capa 2	12	U$ 14,000
Switches Administrables 48 Puertos Capa 2 (24 Puertos 10/100/1000, 4x SFP)	12	U$ 21,000
Switches Administrables 8 Puertos Capa 2 (8 Puertos 10/100/1000)	4	U$ 1,800
Switches Administrables 24 Puertos Capa 3 (8 Puertos 10/100/1000, 16 x SFP)	2	U$ 8,000
UPS 1 KVA Online	20	U$ 22,000
UPS 1.5 KVA Online	2	U$ 3,400
UPS 3 KVA Online	10	U$ 28,000
Router con Acelerador VPN y Lic. SSL de 1 U	4	U$ 14,000
Router con Acelerador VPN y Lic. SSL de 2 U	2	U$ 30,000
SAN fibra canal con doble controladora 4GB	1	U$ 35,400
Cámaras IP	21	U$ 9,400
Impresoras de red	24	U$ 11,000
Wifi	12	U$ 9,000
Relojes Biométricos	4	U$ 4,500
Computadoras completas (CPU, Monitor, Teclado, Ratón, UPS)	280	U$ 252,000

EAAI[101]**:** *Empresa Administradora de Aeropuertos Internacionales.*

Activos Informáticos	Cantidad	Costo Aproximado
Código fuente y ejecutable de los Sistemas de Información (Contabilidad, Nomina, Parqueo, VIP, Tesorería)	1 conjunto	U$ 48,0000
Información de Base de Datos de los sistemas financieros.	1 grupo	U$ 250,000
Respaldos en caja fuerte EAAI y Caja fuerte del Banco	1 grupo	U$ 150,000

Diagrama de dependencia de activos

Una vez identificado los activos se realiza un diagrama de dependencia de activos que demuestra la forma en que todos los activos están interrelacionados y dependientes.

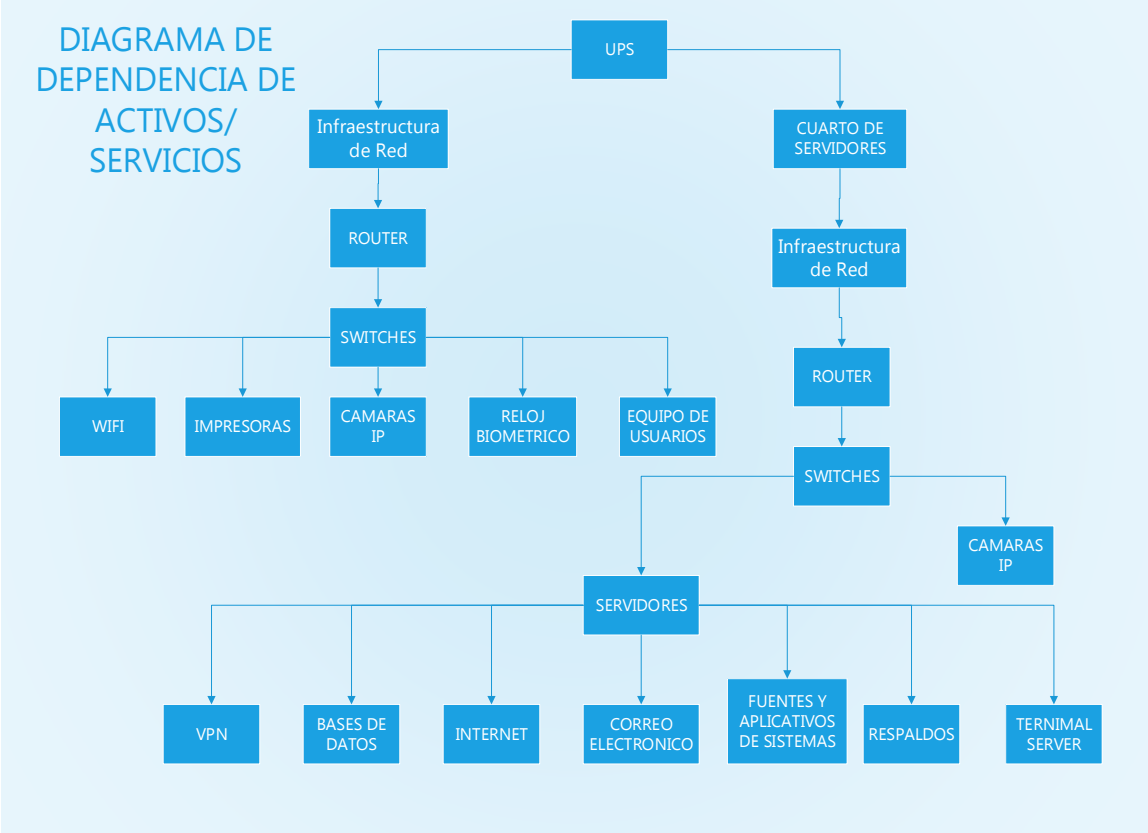


Figura No 12. Diagrama de dependencia de activos.(Desarrollo propio)

En la **Figura No.12. Diagrama de dependencia de activos**, muestra un sin número de elementos de infraestructura de red, ups y servidores que son los elementos vitales para brindar los servicios de la empresa.

A continuación, se presentan los costos de cada uno de los activos descritos en el diagrama de dependencia y de otros que son parte de los servicios de la empresa.

Identificación de los Riesgos asociados a los activos

A partir de la visualización de los activos se procede a enumerar los riesgos, causas y consecuencias. A continuación, las definiciones de los conceptos utilizados durante la enumeración de riesgos los cuales se pueden ver en la **Tabla 2**.

Riesgo: posibilidad de ocurrencia de aquella situación que pueda entorpecer el normal desarrollo de las funciones de la entidad y le impidan el logro de sus objetivos.

Causas (Descripción): se refiere a las características generales o las formas en que se observa o manifiesta el riesgo identificado.

Posibles consecuencias: corresponde a los posibles efectos ocasionados por el riesgo, los cuales se pueden traducir en daños de tipo económico, social, administrativo, entre otros.

Tabla 2. Riesgos asociados a los activos

Riesgo	Causas (Descripción)	Consecuencias
Falta de disponibilidad de sistemas informáticos SIAF[102], Correos Electrónicos y Servicio de Internet por Falla en el fluido eléctrico que podría afectar la reputación y economía de la empresa	Problemas con la planta, Falla de transformador, Se dañó una turbina.	Se agotan las UPS[103] y hay que apagar todo después de 2 Horas de trabajar con respaldo lo cual al perder la disponibilidad de los servicios produce a la empresa perdidas de económicas de U$ 200 por cada hora fuera de servicio y perdidas reputacionales después de 2 días sin servicio.

[102] **SIAF:** *Sistema Integrado Administrativo Financiero.*
[103] **UPS:** *Uninterrumptible Power System, (Sistema de Energía Ininterrumpida).*

Riesgo	Causas (Descripción)	Consecuencias
El Servidor de Producción podría Fallar produciendo falta de disponibilidad de sistemas informáticos impactando económicamente a la empresa al no poder facturar los servicios aeroportuarios.	Se daño el RAID[104], La batería de la cache no funciona bien, Procesadores Recalentados	La Pérdida de conectividad en los sistemas por 3 segundos podría producir pérdidas económicas al momento de registrar transacciones (U$ Monto de Transacción + Costo de Servidor: U$ 13, 000) tanto para la empresa como para los clientes produciendo además problemas reputacionales. Se produce degradación en clúster quedando con un solo equipo.
El hardware del Clúster podría Fallar produciendo perdida de información y económica para la empresa.	Fuerte descarga de energía daña controladoras, Aires acondicionados fallan y no hay internet para monitoreo.	Al dañarse el Clúster se pierden dos horas de información inmediata produciendo falta de disponibilidad de sistemas y dejando un impacto económico de U$ 350 por cada hora sin servicio de los sistemas más el coste del activo dañado (U$ 40,0000).
La posible ocurrencia de daños en equipos de red podría generar pérdidas económicas y falta de disponibilidad de todos los servicios de la empresa.	Rayo afecto equipo y daño varios puertos	Una pérdida de conectividad en el sistema por al menos 30 minutos en caso de no haber disponibilidad para espejo de puertos impactará económicamente a la empresa en un monto de U$ 100 más el costo del activo dañado (U$ 2,500).
Podría efectuarse un ataque a los servidores de correos generando pérdidas económicas, problemas reputacionales y falta de comunicación	Spammers[105] intenta denegación de servicios.	Al no poderse enviar o recibir los correos y al ingresar los IP del servidor en una lista negra imposibilita a la empresa el cumplir con pagos o ingresos urgentes que no podrían ser efectuados. Por ejemplo, el pago de la Nómina. Esta situación de incomunicación produce pérdidas económicas de U$ 120 por cada hora.

[104] **RAID:** *redundant array of independent disks, en español Arreglo redundante de discos independientes.*
[105] **SPAMMERS:** *Termino usado para individuos o empresas que envían correo no deseado.*

Riesgo	Causas (Descripción)	Consecuencias
Al existir la posibilidad de que ocurra una baja en el rendimiento del servicio de internet impactaría económicamente los servicios de la empresa al no poder emitir las facturas a los clientes.	Caída de servicio de un enlace principal del ISP[106], Procesador de Router con demasiados procesos.	Las páginas web abren demasiado lento. Los correos cuestan enviarlos por el tamaño de los adjuntos y el poco ancho de banda produciendo pérdidas económicas de hasta U$100 por hora al no poder enviar de forma inmediata las facturas a los clientes o no poder recibir confirmaciones de transacciones.
Existe la posibilidad de que se conecte a la red personal no autorizado generando posibles fallas en los sistemas que impactarán económicamente la producción de la empresa.	Un trabajador trajo un familiar y le permitió utilizar su equipo y este tenía herramientas de PEN TEST[107].	Un ingreso no autorizado a la red genera falta de disponibilidad de la información produciendo pérdidas económicas de U$ 200 por cada hora perdida.
Los equipos Clientes podrían presentar fallas en sus periféricos produciendo falta de servicio e impactando económicamente a la empresa.	Usuario daño el equipo o dispositivo por descuido derramando alimentos El hardware sufrió daño por años de uso.	El usuario pierde más de 30 minutos de trabajo generando a la empresa pérdidas económicas de hasta U$ 50 por cada 30 minutos.
Podría ocurrir perdida de hardware al fallar Inventario de hardware y software de las PCs[108] generando pérdidas económicas a la empresa.	El software de inventarios dejo de funcionar por falta de un DLL[109] al apagarse mal el equipo.	No hay inventario actualizado. Se puede perder algunos componentes y hasta después de muchos días se darán cuenta. Produciendo así perdidas por el valor del componente extraído siendo las más leves de U$ 150 y las más altas de U$ 500.

[106] **ISP:** *Internet Service Provider, en español proveedor de servicios de internet.*
[107] **PEN TEST:** *Prueba de Penetración de infraestructura de sistemas computacionales.*
[108] **PCs:** *Personal Computers, en español computadoras personales.*
[109] **DLL:** *dynamic-link library, en español biblioteca de enlace dinámico.*

Riesgo	Causas (Descripción)	Consecuencias
El Software antivirus puede dejar de funcionar dejando de proteger los equipos y posibilitando infección de virus a toda la red perjudicando económicamente la empresa.	Una actualización daño un componente del antivirus al no ser compatibles. El usuario ingreso a un sitio web indebido descargando un software que traía un virus que no estaba en la firma por ser amenaza de día 0.	Virus entra en la red y contamina a varios equipos por medio del correo electrónico dejando sin servicio de sistemas a la empresa por dos días e impactando la economía en U$ 800 por cada día perdido.
Pueden ocurrir desastres naturales o provocados por el hombre que inhabiliten parcial o totalmente los servicios de la empresa causando afectación económica.	La ocurrencia de un accidente aéreo que provoca daños en infraestructura del centro de datos y algunos cuartos intermedios.	Perdidas parciales o totales de equipos de comunicaciones de red en cuartos intermedios o principales. El impacto económico del evento es de U$ 350,000.
	Se lleva a cabo la combustión por una explosión provocada por falla en panel eléctrico. El transformador principal se daña y envía 4 veces más voltaje del requerido.	Pérdida parcial o total de servidores y Core de internet de la empresa. El impacto económico de este evento que afecta los servicios de internet, sistemas y todo lo que depende de la red es de U$ 250,000.
	Se activa las fallas que pasa en el aeropuerto y daña totalmente la terminal aérea y la Pista de aterrizaje. Desaparecen todos los edificios.	Se produce perdida de disponibilidad de servicios y de información con un efecto económico negativo de al menos U$ 300, 000 en equipos y U$ 250,000 en daños a edificios e infraestructuras.
	Un exceso de caudal de los desagües produce inundación de oficinas XY	Los daños mínimos por inundación pueden ser de U$ 20,000.

Riesgo	Causas (Descripción)	Consecuencias
Podrían causarse daños en cableados de Fibra Óptica en ductería existente en tesorería o Facturación Crédito afectando la disponibilidad de los sistemas y causando perdías económicas.	Personal externo realiza acometida de F.O.[110] OM3[111] dañando al momento de sondear otras fibras instaladas.	Se daña un cable F.O.[110] y se pierde conectividad de unas áreas que generan ingresos y producen perdidas de al menos U$ 1,000 por cada día más el costo de la reparación de la Fibra óptica (De U$ 700 a U$ 1500)
	Personal de Mantenimiento realizando una obra de zanjeo daña tubería de canalizaciones de Fibra Óptica.	

Determinación del impacto

Para determinar el impacto es importante ver el tema de la magnitud del daño si el riesgo se llegara a materializar. Estimar la Magnitud de Daño generalmente es una tarea muy compleja. La manera más fácil es expresar el daño de manera cualitativa, lo que significa que aparte del daño económico, por lo que veremos un historial de los daños registrados, de igual manera se considera otros valores como daños de imagen, emocionales, entre otros. Expresarlo de manera cuantitativa, es decir calcular todos los componentes en un solo daño económico, resulta en un ejercicio aún más complejo y extenso. Durante todo el proceso del análisis de riesgos utilizamos en primera instancia la **Tabla 3** (Datos para cálculos económicos en base a ocurrencias históricas de la empresa). El siguiente paso es determinar controles para cada riesgo encontrado. La **Tabla 4** (Riesgos y Controles con sus probabilidades, impactos y degradación cualitativa.) muestra un análisis cualitativo y en la **Tabla 5** (Calificaciones de Riesgos, Controles, Salvaguardas, Ocurrencia, Efectividad y Riesgo económico) se expone un análisis cuantitativo de los riesgos y se prueban los controles.

[110] **F.O.:** *Fibra Óptica*
[111] **OM3:** *Cable de Fibra Óptica con velocidades de 10 Gbps a una distancia de 300 mts*

Tabla 3. Datos para cálculos económicos en base a ocurrencias históricas de la empresa

Datos Registrados	Cantidad	Costos
Fuentes de poder dañadas al año	15	$525,00
Ups 750 VA[112] dañadas al año	2	$240,00
Estabilizador de 3000 Watts dañados en 5 años	1	$800,00
Acumuladores dañados al año	25	$625,00
Daño de Controladora RAID[113] en 5 años	1	$800,00
Daño de batería de cache en 5 años	1	$250,00
Respaldos no trasladados cada dos horas en un año	5	$58.649,38
Falla en Servidor Virtual en 5 años	1	$11.729,88
Falla de un Switch en 5 años	3	$4.500,00
Servicio de Internet falla (suplir con modem 3g) en 5 años	2	$300,00
Servidor de Correos Bloqueado Lista Negra en 5 años (Suplir con llamadas)	3	$225,00
Falla de un Router en 5 años	1	$3.500,00
Daños en UPS[114] online de 1 Kva[115] en 5 años	1	$1.100,00
Daños en UPS[114] online de 1,5 Kva[115] en 5 años	1	$1.700,00
Daños en UPS[114] online de 3 Kva[115] en 5 años	1	$2.800,00
Teclados dañados al año	1	$14,00
Ratón Dañados al año	2	$14,00
Costo de Contratar para PEN TEST[116]	1	$3.000,00
Impresora Láser dañada en 5 años	1	$450,00
Impresora Matricial dañada en 5 años	1	$300,00
Costo por perder o dañar Módulo de memoria de 1 GB en 5 años	2	$80,00
Costo de Horas hombre por reinstalar sistema operativo y todos sus componentes (antivirus se dañó) ocurrencia anual.	2	$120,00
Costo por activación de sistema INERGEN 5 cilindros descargados, ocurrencia 10 años	1	$5.750,00
Daño en infraestructura de edificios, pistas, mobiliario y equipo, maquinaria. Ocurrencia 40 años	1	$216.666.666,67
Equipos de reposición por contingencia	2	$1.800,00
Costo de Acometida de Fibra Óptica entre 200 y 300 metros	1	$5.000,00

[112] **VA:** *Termino usado para hablar de voltiamperio*
[113] **RAID:** *Redundant array of independent disks, en español Arreglo redundante de discos independientes.*
[114] **UPS:** *Uninterrumptible Power System, (Sistema de Energía Ininterrumpida).*
[115] **KVA:** *Termino usado para hablar de kilovoltiamperio*
[116] **PEN TEST:** *Prueba de Penetración de infraestructura de sistemas computacionales.*

Matriz de Riesgos

Para el desarrollo de la matriz de riesgos se definen tres elementos: Probabilidad de Ocurrencia, Impacto del Riesgo y Degradación del valor del activo.

Degradación del Valor

1	Muy Baja
2	Baja
3	Media
4	Alta
5	Muy Alta

Probabilidad de Ocurrencia

1	Muy poco frecuente
2	Poco Frecuente
3	Normal
4	Frecuente
5	Muy Frecuente

Impacto del Riesgo

1	No provoca daños
2	El daño es menor
3	El daño es moderado
4	El daño es mayor
5	El daño es catastrófico

Tabla 4. Riesgos y Controles con sus probabilidades, impactos y degradación cualitativa.

No	Riesgo	Degradación de valor	Probabilidad	Impacto	Controles	Causas (Descripción)
1	**R1:** Falta de disponibilidad de sistemas informáticos SIAF, Correos Electrónicos y Servicio de Internet por Falla en el fluido eléctrico que podría afectar la reputación y economía de la empresa	2	3	4	**C1:** Gerencia de TI por medio del área de infraestructura y soporte técnico garantiza el uso de UPS con bancos Online (UPS Online de 16 KVA, 3 KVA, 1 KVA, 750 VA) en cada dispositivo de red, Servidores y Equipos Clientes. A demás reguladores de voltajes para impresoras.	Problemas con la planta, Falla de transformador, Se dañó una turbina. Falla energía convencional del proveedor UNION FENOSA Vehículo daña poste de energía al chochar y provoca corte de luz.
2	**R2:** El Servidor de Producción podría Fallar produciendo falta de disponibilidad de sistemas informáticos impactando económicamente a la empresa al no poder facturar los servicios aeroportuarios.	3	3	2	**C2:** El área de Infraestructura tiene configurada y administra un Clúster de Servidores que permite de forma automática intercambiar roles de servidores activo/Pasivo garantizando la disponibilidad del SIAF[117].	Se daño el RAID, La batería de la cache no funciona bien, Procesadores Recalentados

[117] **SIAF:** *Sistema Integrado Administrativo Financiero.*

No	Riesgo	Degradación de valor	Probabilidad	Impacto	Controles	Causas (Descripción)
3	**R3:** El hardware del Clúster podría Fallar produciendo perdida de información y económica para la empresa.	4	2	4	**C3:** El jefe de infraestructura de Red y Base de datos tiene mecanismos de respaldos (Backup[118] cada dos horas) fuera del clúster que son luego copiados a un servidor virtual de Backup[118] para garantizar la disponibilidad de los sistemas al fallar el clúster.	Fuerte descarga de energía daña controladoras, Aires acondicionados fallan y no hay internet para monitoreo. Se daña la batería de la cache de la RAID y se corrompe la configuración de los arreglos.
4	**R4:** La posible ocurrencia de daños en equipos de red podría generar pérdidas económicas y falta de disponibilidad de todos los servicios de la empresa.	3	2	4	**C4:** Gerencia de TI[119] por medio del área de infraestructura de redes posee Router, Switches de capa 2 y 3 de respaldos para sustituir equipos dañados	Rayo afecto Switch de forma parcial (Daño de algunos puertos) o total. Router se dañó por funcionamiento continuo de forma parcial o total.
5	**R5:** Podría efectuarse un ataque a los servidores de correos generando pérdidas económicas, problemas reputacionales y falta de comunicación	2	4	4	**C5:** El personal de infraestructura administra un IPS[120] que realiza bloqueos proactivos ante ataques a servidores de correos y equipos de red.	Spammers[121] intenta denegación de servicios.

[118]**Backup:** *Respaldos*
[119]**TI:** *Tecnologías de la Información*
[120]**IPS:** Intrusion Prevention System, en español Sistema de Prevención de Intrusos.
[121]**SPAMMERS:** *Termino usado para individuos o empresas que envían correo no deseado.*

	Riesgo	Degradación de valor	Probabilidad	Impacto	Controles	Causas (Descripción)
6	**R6:** Al existir la posibilidad de que ocurra una baja en el rendimiento del servicio de internet impactaría económicamente los servicios de la empresa al no poder emitir las facturas a los clientes.	1	2	3	**C6:** Soporte Técnico de Infraestructura de Red monitorea por medio de SolarWinds NetWorkMonitor Memoria, CPU[122] y tráfico del Router principal y Switch Core para asegurar funcionamiento correcto bloqueando conexiones extrañas en el tráfico analizado.	Caída de servicio de un enlace principal del ISP[123], Procesador de Router con demasiados procesos. Se efectúa ataque de Denegacion de Servicios (DoS[124]) o intento de intrusión a la red.
7	**R7:** Existe la posibilidad de que se conecten a la red personal no autorizado generando posibles fallas en los sistemas que impactarán económicamente la producción de la empresa.	2	2	4	**C7:** El personal de soporte técnico de infraestructura monitorea Tráfico con WireShark para validar los protocolos usados Y Planifica un Checklist[125] por áreas para validar software instalado y accesos.	Un trabajador trajo un familiar y le permitió utilizar su equipo y este tenía herramientas de PEN TEST[126].

[122]**CPU:** *central processing unit, en español unidad central de procesamiento.*
[123]**ISP:** *Internet Service Provider, en español proveedor de servicios de internet.*
[124]**DoS:** *Denial of Service, en español denegación de servicio*
[125]**Checklist:** *lista de tareas predefinida.*
[126]**PEN TEST:** *Prueba de Penetración de infraestructura de sistemas computacionales.*

No	Riesgo	Degradación de valor	Probabilidad	Impacto	Controles	Causas (Descripción)
8	**R8:** Los equipos Clientes podrían presentar fallas en sus periféricos produciendo falta de servicio e impactando económicamente a la empresa.	2	2	4	**C8:** La Gerencia de TI[127] por medio del manual de uso de equipos y medios informáticos está facultada para emitir memorando con sanciones administrativas y cobros por daños a equipos y medios informáticos. **C9:** Personal de Soporte Técnico posee de respaldo Fuentes de Poder, teclado, ratón y periféricos para ser utilizados cuando se requiera.	Usuario daño el equipo o dispositivo por descuido derramando alimentos Se daño por uso normal del equipo. Factores de orden tecnológico o fortuito.
9	**R9:** Podría ocurrir perdida de hardware al fallar Inventario de hardware y software de las PCs[128] generando pérdidas económicas a la empresa.	1	2	2	**C10:** Personal de Soporte Técnico es encargado de validar visor de sucesos y consola de servidor de inventarios para saber qué equipo no está reportando inventario.	El software de inventarios dejo de funcionar por falta de un DLL[129] al apagarse mal el equipo.
10	**R10:** El Software antivirus puede dejar de funcionar dejando de proteger los equipos y posibilitando infección de virus a toda la red perjudicando económicamente la empresa.	2	2	3	**C11:** El jefe de soporte técnico monitorea el servidor de antivirus para saber si todos los equipos se están actualizando bien. **C12:** Personal de soporte técnico realiza Checklist periódico en periodos de mantenimiento preventivo.	Una actualización daño un componente del antivirus al no ser compatibles

[127] **TI:** *Tecnologías de la Información.*
[128] **PCs:** *Personal Computers, en español computadoras personales.*
[129] **DLL:** *dynamic-link library, en español biblioteca de enlace dinámico.*

No	Riesgo	Degradación de valor	Probabilidad	Impacto	Controles	Causas (Descripción)
11	**R11:** Pueden ocurrir desastres naturales o provocados por el hombre que inhabiliten parcial o totalmente los servicios de la empresa causando afectación económica.	5	2	5	**C13:** El aeropuerto cuenta con un Sistema de Supresión de incendios automatizado que administran los bomberos y monitorea Gerencia de TI.	Se lleva a cabo la combustión por una explosión provocada por falla en panel eléctrico. El transformador principal se daña y envía 4 veces más voltaje del requerido.
		5	3	5	**C14:** El aeropuerto cuenta con un Plan de Emergencias ante desastres naturales o provocados que es dirigido por el Comité de Emergencia encabezado por el Gerente General.	Se activa las fallas que pasa en el aeropuerto y daña totalmente la terminal aérea y la Pista de aterrizaje. Desaparecen todos los edificios.
		3	3	4	**C15:** Personal de Seguridad aeroportuaria monitorea las 24 horas las cámaras de vigilancia. **C16:** El aeropuerto cuenta con una Oficina de Contingencia administrada por recursos humanos.	Un exceso de caudal de los desagües produce inundación de oficinas XY

No	Riesgo	Degradación de valor	Probabilidad	Impacto	Controles	Causas (Descripción)
12	**R12:** Podrían causarse daños en cableados de Fibra Óptica en ductería existente en tesorería o Facturación Crédito afectando la disponibilidad de los sistemas y causando perdías económicas.	3	2	4	**C17:** Supervisión de Gerencia de TI en toda actividad de cableado.	Personal externo realiza instalación de nuevo cableado OM3[130] y perjudica por accidente un cable de fibra en uso.

[130] **OM3:** *Cable de Fibra Óptica con velocidades de 10 Gbps a una distancia de 300 mts.*

Tabla 5. Calificaciones de Riesgos, Controles, Salvaguardas, Ocurrencia, Efectividad y Riesgo económico.

No	Riesgo	**R1:** Falta de disponibilidad de sistemas informáticos SIAF, Correos Electrónicos y Servicio de Internet por Falla en el fluido eléctrico que podría afectar la reputación y economía de la empresa			
	Controles	**C1:** Gerencia de TI por medio del área de infraestructura y soporte técnico garantiza el uso de UPS con bancos Online (UPS Online de 16 KVA, 3 KVA, 1 KVA, 750 VA) en cada dispositivo de red, Servidores y Equipos Clientes. A demás reguladores de voltajes para impresoras.			
	Causas (Descripción)	**Ocurrencia (R=N/T)**	**Efectividad del Control (F/S)X100**	**Riesgo Económico (Re=ExF) F=1/T**	**Salvaguardas**
1	Problemas con la planta, Falla de transformador, Se dañó una turbina.	N= 3 T = 1825 R=3/1825=0,00164	F= 1822 S=1825 (1822/1825)X100 = 99,84 %	F= 1/5=0,2 E=(1100+1700 +2800) Re=(U$ 5600x0,2)= U$ 1120 / año	HW Protección de los Equipos Informáticos.
	Falla energía convencional del proveedor UNION FENOSA	N= 42 T = 365 R=42/365=0,1151	F= 323 S=365 (323/365)X100= 88,49 %	F= 1/1=1 E=(240+625+525) Re=(U$ 1390x1)= U$ 1390 / año	COM Protección de las Comunicaciones.
	Vehículo daña poste de energía al chochar y provoca corte de luz.	N= 1 T = 365 R=1/365=0,0027	F= 364 S=365 (364/365)X100= 99,73 %	F= 1/5=0,2 E=(800) Re=(U$ 800x0,2)= U$ 160 / año	

No	**Riesgo**	**R2:** El Servidor de Producción podría Fallar produciendo falta de disponibilidad de sistemas informáticos impactando económicamente a la empresa al no poder facturar los servicios aeroportuarios.			
2	**Controles**	**C2:** El área de Infraestructura tiene configurada y administra un Clúster de Servidores que permite de forma automática intercambiar roles de servidores activo/Pasivo garantizando la disponibilidad del SIAF[131].			
	Causas (Descripción)	**Ocurrencia (R=N/T)**	**Efectividad del Control (F/S)X100**	**Riesgo Económico (Re=ExF) F=1/T**	**Salvaguardas**
	Se dañó el RAID, La batería de la cache no funciona bien, Procesadores Recalentados	N= 2 T = 1825 R=2/1825=0,0011	F= 1823 S=1825 (1823/1825)X100 = 99,89 %	F= 1/5=0,2 E=(800+250) Re=(U$ 1050x0,2)= U$ 210 / año	D.A Copias de seguridad de los datos (Backup).

[131] **SIAF:** *Sistema Integrado Administrativo Financiero.*

No	Riesgo	**R3:** El hardware del Clúster podría Fallar produciendo perdida de información y económica para la empresa.			
3	**Controles**	**C3:** El jefe de infraestructura de Red y Base de datos tiene mecanismos de respaldos (Backup cada dos horas) fuera del clúster que son luego copiados a un servidor virtual de Backup para garantizar la disponibilidad de los sistemas al fallar el clúster.			
	Causas (Descripción)	**Ocurrencia (R=N/T)**	**Efectividad del Control (F/S)X100**	**Riesgo Económico (Re=ExF) F=1/T**	**Salvaguardas**
	Fuerte descarga de energía daña controladoras, Aires acondicionados fallan y no hay internet para monitoreo.	N= 5 T = 1825 R=1/1825=0,00274	F= 1820 S=1825 (1820/1825)X100 = 99,72 %	F= 1/5=0,2 E=(58649,38) Re= (U$ 58649,38x0,2) = U$ 11729,88 / año	D.I Aseguramiento de la integridad
	Se daña la batería de la cache de la RAID y se corrompe la configuración de los arreglos.	N= 1 T = 1825 R=1/1825=0,00055	F= 1824 S=1825 (1824/1825)X100 = 99,94 %	F= 1/5=0,2 E=(11729,88) Re=(U$ 11729,88x0,2)= U$ 210 / año	SW.A Copias de seguridad (backup)

No	Riesgo	**R4:** La posible ocurrencia de daños en equipos de red podría generar pérdidas económicas y falta de disponibilidad de todos los servicios de la empresa.			
4	Controles	**C4:** Gerencia de TI por medio del área de infraestructura de redes posee Router, Switches de capa 2 y 3 de respaldos para sustituir equipos dañados.			
	Causas (Descripción)	**Ocurrencia (R=N/T)**	**Efectividad del Control (F/S)X100**	**Riesgo Económico (Re=ExF) F=1/T**	**Salvaguardas**
	Rayo afecto Switch de forma parcial (Daño de algunos puertos) o total.	N= 3 T = 1825 R=3/1825=0,00164	F= 1822 S=1825 (1822/1825)X100= 99,84 %	F= 1/5=0,2 E=(4500) Re=(U$ 4500x0,2)= U$ 900 / año	COM Protección de las Comunicaciones
	Router se dañó por funcionamiento continuo de forma parcial o total.	N= 1 T = 1825 R=1/1825=0,00055	F= 1824 S=1825 (1824/1825)X100= 99,95 %	F= 1/5=0,2 E=(3500) Re=(U$ 3500x0,2)= U$ 700 / año	COM.A Aseguramiento de la disponibilidad

No	**Riesgo**	**R5:** Podría efectuarse un ataque a los servidores de correos generando pérdidas económicas, problemas reputacionales y falta de comunicación			
5	**Controles**	**C5:** El personal de infraestructura administra un IPS que realiza bloqueos proactivos ante ataques a servidores de correos y equipos de red.			
	Causas (Descripción)	**Ocurrencia (R=N/T)**	**Efectividad del Control (F/S)X100**	**Riesgo Económico (Re=ExF) F=1/T**	**Salvaguardas**
	Spammers intenta denegación de servicios.	N= 3 T = 1825 R=3/1825=0,00164	F= 1822 S=1825 (1822/1825)X100 = 99,84 %	F= 1/5=0,2 E=(225) Re=(U$ 225x 0,2)= U$ 45 / año	H.tools.IDS IDS/IPS: Herramienta de detección / prevención de intrusión

No	Riesgo	**R6:** Al existir la posibilidad de que ocurra una baja en el rendimiento del servicio de internet impactaría económicamente los servicios de la empresa al no poder emitir las facturas a los clientes.			
6	Controles	**C6:** Soporte Técnico de Infraestructura de Red monitorea por medio de SolarWinds NetWorkMonitor Memoria, CPU y tráfico del Router principal y Switch Core para asegurar funcionamiento correcto bloqueando conexiones extrañas en el tráfico analizado.			
	Causas (Descripción)	**Ocurrencia (R=N/T)**	**Efectividad del Control (F/S)X100**	**Riesgo Económico (Re=ExF) F=1/T**	**Salvaguardas**
	Caída de servicio de un enlace principal del ISP, Procesador de Router con demasiados procesos.	N= 2 T = 1825 R=2/1825= 0,0011	F= 1823 S=1825 (1823/1825)X100= 99,89 %	F= 1/5=0,2 E=(300) Re=(U$ 300x 0,2)= U$ 60 / año	H.tools.TM Herramienta de monitorización de tráfico
	Se efectúa ataque de Denegación de Servicios (DoS) o intento de intrusión a la red.	N= 5 T = 1825 R=5/1825= 0,0027	F= 1822 S=1825 (1822/1825)X100= 99,84 %	F= 1/5=0,2 E=(300) Re=(U$ 300x 0,2)= U$ 60 / año	H.tools.LA Herramienta para análisis de logs

No	**Riesgo**	**R7:** Existe la posibilidad de que se conecten a la red personal no autorizado generando posibles fallas en los sistemas que impactarán económicamente la producción de la empresa.			
7	**Controles**	**C7:** El personal de soporte técnico de infraestructura monitorea Tráfico con WireShark para validar los protocolos usados y planifica un Checklist por áreas para validar software instalado y accesos.			
	Causas (Descripción)	**Ocurrencia (R=N/T)**	**Efectividad del Control (F/S)X100**	**Riesgo Económico (Re=ExF) F=1/T**	**Salvaguardas**
	Un trabajador trajo un familiar y le permitió utilizar su equipo y este tenía herramientas de PEN TEST.	N= 1 T = 1825 R=1/1825= 0,00055	F= 1824 S=1825 (1824/1825)X100 = 99,94 %	F= 1/5=0,2 E=(3000) Re=(U$ 3000x 0,2)= U$ 600 / año	H.tools.VA Herramienta de análisis de vulnerabilidades
No	**Riesgo**	**R8:** Los equipos Clientes podrían presentar fallas en sus periféricos produciendo falta de servicio e impactando económicamente a la empresa.			
8	**Controles**	**C8:** La Gerencia de TI por medio del manual de uso de equipos y medios informáticos está facultada para emitir memorando con sanciones administrativas y cobros por daños a equipos y medios informáticos. **C9:** Personal de Soporte Técnico posee de respaldo Fuentes de Poder, teclado, ratón y periféricos para ser utilizados cuando se requiera.			
	Causas (Descripción)	**Ocurrencia (R=N/T)**	**Efectividad del Control (F/S)X100**	**Riesgo Económico (Re=ExF) F=1/T**	**Salvaguardas**
	Usuario daño el equipo o dispositivo por descuido derramando alimentos	N= 5 T = 1825 R=5/1825= 0,0027	F= 1820 S=1825 (1823/1825)X100 = 99,73 %	F= 1/5=0,2 E= (450+350+14+14 +35) Re=(U$ 863x 0,2)= U$ 172,6 / año	PS Gestión del Personal
	Se daño por uso normal del equipo. Factores de orden tecnológico o fortuito.				PS.AT Formación y concienciación

No	**Riesgo**	**R9:** Podría ocurrir perdida de hardware al fallar Inventario de hardware y software de las PCs generando pérdidas económicas a la empresa.			
9	**Controles**	**C10:** Personal de Soporte Técnico es encargado de validar visor de sucesos y consola de servidor de inventarios para saber qué equipo no está reportando inventario.			
	Causas (Descripción)	**Ocurrencia (R=N/T)**	**Efectividad del Control (F/S)X100**	**Riesgo Económico (Re=ExF) F=1/T**	**Salvaguardas**
	El software de inventarios dejo de funcionar por falta de un DLL al apagarse mal el equipo.	N= 2 T = 1825 R=2/1825=0,0011	F= 1823 S=1825 (1823/1825)X100= 99,89 %	F= 1/5=0,2 E=(80) Re=(U$ 80x 0,2)= U$ 16 / año	S.CM Gestión de cambios (mejoras y sustituciones)
No	**Riesgo**	**R10:** El Software antivirus puede dejar de funcionar dejando de proteger los equipos y posibilitando infección de virus a toda la red perjudicando económicamente la empresa.			
10	**Controles**	**C11:** El jefe de soporte técnico monitorea el servidor de antivirus para saber si todos los equipos se están actualizando bien. **C12:** Personal de soporte técnico realiza Checklist periódico en periodos de mantenimiento preventivo.			
	Causas (Descripción)	**Ocurrencia (R=N/T)**	**Efectividad del Control (F/S)X100**	**Riesgo Económico (Re=ExF) F=1/T**	**Salvaguardas**
	Una actualización daño un componente del antivirus al no ser compatibles	N= 2 T = 365 R=2/365=0,0055	F= 1823 S=1825 (1823/1825)X100= 99,89 %	F= 1/5=0,2 E=(120) Re=(U$ 80x 0,2)= U$ 16 / año	H.IR Gestión de incidencias

No	Riesgo	R11: Pueden ocurrir desastres naturales o provocados por el hombre que inhabiliten parcial o totalmente los servicios de la empresa causando afectación económica.			
11	Controles	**C13:** El aeropuerto cuenta con un Sistema de Supresión de incendios automatizado que administran los bomberos y monitorea Gerencia de TI. **C14:** El aeropuerto cuenta con un Plan de Emergencias ante desastres naturales o provocados que es dirigido por el Comité de Emergencia encabezado por el Gerente General. **C15:** Personal de Seguridad aeroportuaria monitorea las 24 horas las cámaras de vigilancia. **C16:** El aeropuerto cuenta con una Oficina de Contingencia administrada por recursos humanos.			
	Causas (Descripción)	**Ocurrencia (R=N/T)**	**Efectividad del Control (F/S)X100**	**Riesgo Económico (Re=ExF) F=1/T**	**Salvaguardas**
	Combustión por una explosión provocada por falla en panel eléctrico. El transformador principal se daña y envía 4 veces más voltaje del requerido.	N= 1 T = 3650 R=1/3650= 0,00027	F= 3649 S=3650 (3649/3650)X100= 99,97 %	F= 1/10=0,1 E=(5750) Re=(U$ 5750x 0,2)= U$ 575 / año	H Protecciones Generales G.RM Gestión de riesgos
	Se activa las fallas que pasa en el aeropuerto y daña totalmente la terminal aérea y la Pista de aterrizaje. Desaparecen todos los edificios.	N= 1 T = 14600 R=2/365= 0,000068	F= 14597 S=14600 (14597/14600) X100= 99,97 %	F= 1/40=0,025 E=(216666666,67) Re=(U$ 216666666x 0,025)= U$ 5416666,67 / año	G.RM Gestión de riesgos
	Un exceso de caudal de los desagües produce inundación de oficinas XY	N= 3 T = 1825 R=3/1825= 0,0016	F= 1822 S=1825 (1822/1825)X100= 99,84 %	F= 1/5=0,2 E=(1800) Re=(U$ 1800x 0,2)= U$ 360 / año	G.RM Gestión de riesgos

No	Riesgo	**R12:** Podrían causarse daños en cableados de Fibra Óptica en ductería existente en tesorería o Facturación Crédito afectando la disponibilidad de los sistemas y causando perdías económicas.			
	Controles	**C17:** Supervisión de Gerencia de TI en toda actividad de cableado.			
12	**Causas (Descripción)**	**Ocurrencia (R=N/T)**	**Efectividad del Control (F/S)X100**	**Riesgo Económico (Re=ExF) F=1/T**	**Salvaguardas**
	Personal externo realiza instalación de nuevo cableado OM3 y perjudica por accidente un cable de fibra en uso.	N= 1 T = 1825 R=1/1825=0,00055	F= 1824 S=1825 (1824/1825)X100= 99,94 %	F= 1/5=0,2 E=(5000) Re=(U$ 5000x 0,2)= U$ 1000 / año	PS.A Aseguramiento de la disponibilidad

7.2. ANÁLISIS DE LA TOPOLOGÍA DE LA RED

El análisis de los riesgos a los que los principales activos de la empresa están expuesto y que fueron mencionados con anterioridad nos da a primera mano una clasificación de todos los activos que son de vital importancia para la empresa y que a su vez consumen y producen algún tipo de información. En el caso de este trabajo que se desarrolla el principal elemento de información que es de utilidad son todos los LOG generados por los dispositivos de red y servidores. Para entender como está diseñada la red se mostrará un diagrama denominado "**Figura No13**. Diagrama de Situación actual de la Red" en donde se muestran las principales conexiones. Por efectos de protección de la información de la empresa no se ofrecerá la descripción completa de todos los equipos y sus conexiones. De igual forma los modelos no son los mismos implementados en la empresa.

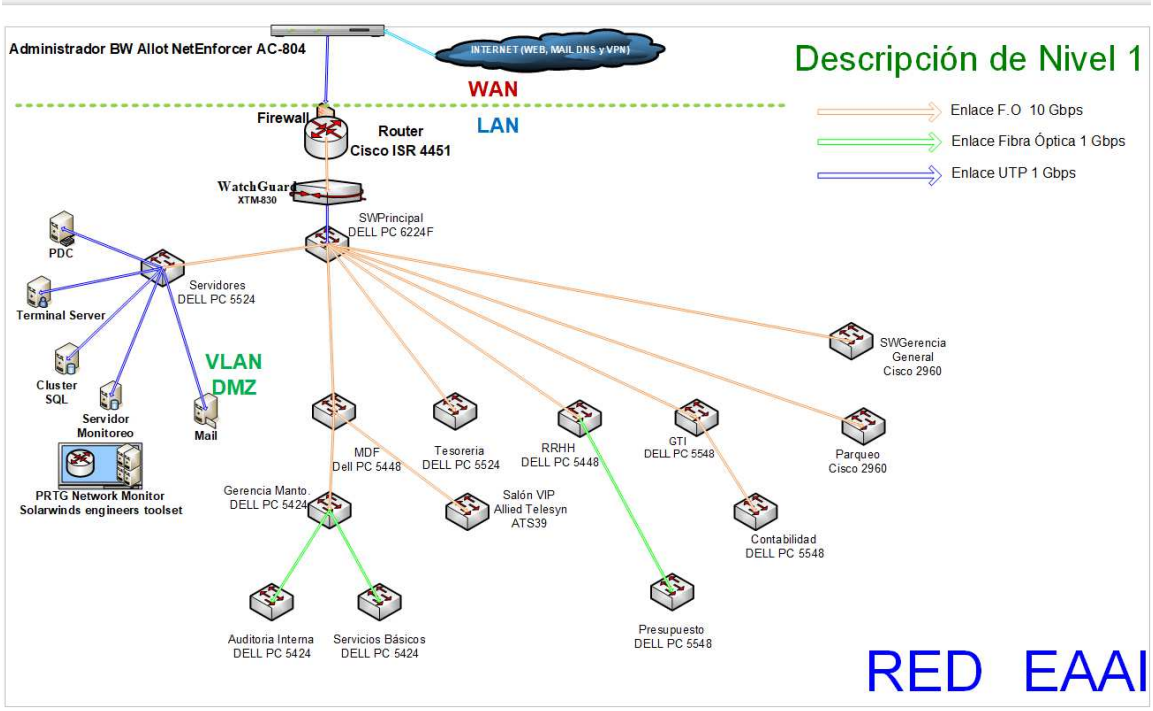


Figura No 13 Diagrama de Situación actual de la Red. (Desarrollo propio)

En este escenario de la **Figura N13**. Se puede observar que la empresa recibe el servicio de internet provisto por el ISP directamente a un equipo administrador de ancho de banda marca Allot; este equipo no solo administra el ancho de

banda sino también tiene integrado una opción de protección contra ataques de denegación de servicios (DoS, Deny of Service). El equipo Allot NetEnforcer entrega el ancho de banda que se desea al Router principal de la EAAI que es un Cisco. Ese equipo Cisco posee firewall. El cisco que es la frontera entre al WAN[132] y la LAN[133] de la empresa no está conectado directamente a la LAN[133]. El Cisco está conectado a un UTM[134] Watchguard que posee firewall, antivirus, filtro URL, IPS, AntiSpam y QoS[135] para manejo de ancho de banda interno. El WatchGuard está conectada a un Switch Principal de 24 Puertos de Fibra Óptica. Posterior a esa conexión toda la topología es de estrella con redundancia en enlaces críticos. La cantidad de equipos conectados son más de 400 incluyendo servidores, cámaras, relojes biométricos, equipos de red y seguridad perimetral. Los log son administrados de forma independiente.

[132]**WAN:** *Wide Area Network, en español Red de Área Amplia.*
[133]**LAN:** *Local Area Network, en español Red de Área Local*.
[134]***UTM:*** Unified threat management; en español Gestión unificada de amenazas.
[135]**QoS:** *quality of service, en español calidad de servicio*

7.3. ADECUACIONES DE INFRAESTRUCTURA TECNOLÓGICA DE LA EAAI

La topología de red mostrada con anterioridad nos brinda una visión completa de que elementos se deben adecuar para la implementación de un SIEM[136] en la empresa. En este caso para aumentar los niveles de certeza de los ataques se pueden implementar equipos con software Open Source en la parte WAN como un SNORT en modo IPS. A nivel LAN se puede configurar un equipo previo al SIEM que recoja los LOG de los servidores de Correos y DNS (Servidor de Nombres de Dominio). El equipo a implementarse puede hacer uso de rsyslog y utilizar un Centos 7. Con el equipo de SysLog se tendrá log de los servidores sin perjudicar el funcionamiento de los mismos y comprometer su seguridad al instalar agentes o universal forwarders (reenviadores universales). Una vez instalado el universal forwarder se estarán enviando los log al SIEM[136] que se tenga configurado. A Continuación se muestra el diagrama propuesto para la integración de un SIEM[136].

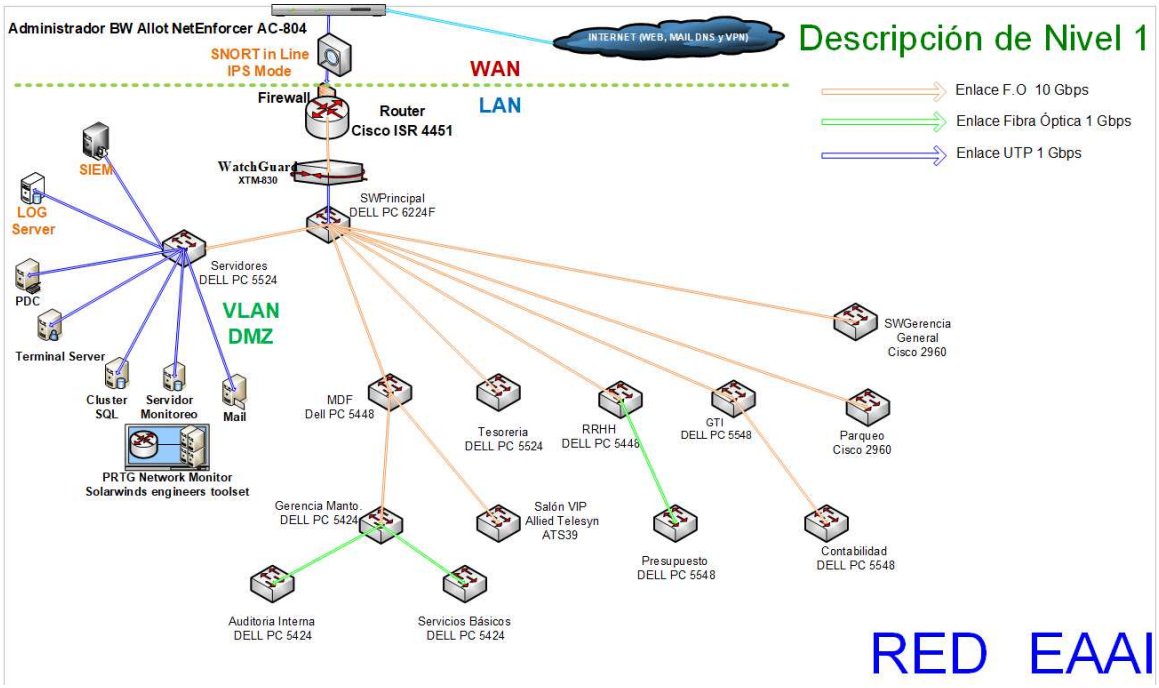


Figura No 14. Diagrama de Situación deseada de la Red para implementar SIEM. (Desarrollo Propio)

[136]**SIEM:** *Security Information and Event Management, en español conocido como Sistema de Gestión de Eventos de Seguridad de la Información*

En el diagrama de la **Figura No14** se puede observar que cualquier equipo dentro de la LAN que genera LOG puede enviar sus registros a un servidor de LOG o al SIEM. Esto en dependencia del nivel de configuración a ser aplicada en los equipos que producen LOG. En caso por ejemplo de servidores como antivirus que tengan integrado su propia herramienta de direccionamiento de LOG solo se brindará el IP del servidor syslog. En caso de no poseer algún método de reenvío se puede instalar el agente que proporciona la solución SIEM para obtener los LOG del servidor; puede por ejemplo ser integrado de esta forma un servidor de Windows. De igual forma por cuestiones de seguridad y estabilidad de servidores como el de correos se recomienda no instalar ningún agente de un SIEM sino reenviar los LOG al servidor de propuesto para ese. De esa forma garantizamos el buen desempeño de los recursos de la red durante cualquier implementación.

7.4. IDENTIFICACIÓN DE CONTROLES CRÍTICOS

Identificación de controles implementados y determinación de su efectividad.

Es importante destacar que los riesgos y/o amenazas ligadas a los activos son aplicadas y válidas para salvaguardar cualquier servicio que la EAAI ofrezca o sea necesario para su continuidad de negocio.

A partir de esta visión general de cómo se relacionan los activos de la empresa se ha procedido a establecer una tabla que contiene para cada riesgo uno o más controles asociados. Elementos que son usados en los diagramas de flujo de procesos en estudio.

Ver la **Tabla 6**. Determinación de Efectividad de los Controles. Donde el campo NR es el número de riesgo evaluado con sus controles y es equivalente al número de riesgos y controles de según la **Tabla 4**.

Tabla 6. Determinación de efectividad de los controles.

NR	CONTROL A EVAULAR
1	**C1:** Gerencia de TI por medio del área de infraestructura y soporte técnico garantiza el uso de UPS con bancos Online (UPS Online de 16 KVA, 3 KVA, 1 KVA, 750 VA) en cada dispositivo de red, Servidores y Equipos Clientes. A demás reguladores de voltajes para impresoras.
	Fuente del Riesgo: Entorno, **Tipo de Riesgo:** Riesgo de Proceso
	Pruebas Operativas
	Se verificó la existencia de UPS de respaldo de distintas capacidades. A demás se encontraron acumuladores de respaldos para las UPS activas.
	Se visitó con apoyo de personal de soporte técnico y de infraestructura las áreas de servidores, cuartos intermedios y oficinas de clientes constatando la presencia de UPS y su correcto funcionamiento.
	Se observó en documentos de mantenimientos el proceso de verificación de las UPS en cada visita técnica.
	Pruebas de Diseño
	¿Están diseñados correctamente los controles? El control está diseñado correctamente ya que en dependencia del equipo activo se tienen distintos UPS de capacidades variables y reguladores de voltaje para impresoras.
	¿El que ejecuta cada control es el adecuado? Se encuentra adecuada la ejecución del control puesto que el personal encargado de vigilar las UPS de los clientes es el personal de soporte técnico y el de los servidores y equipos de la red es el personal de infraestructura de red y base de datos.
	¿Se ejecuta cada control en el momento adecuado? Efectivamente se demostró en sitio que al momento de una falla energética las UPS brindan la autonomía de respaldo requerida para salvaguardar la información y garantizar que finalice con éxito la transacción que este en el momento del incidente.
	¿Hay evidencia que los controles se están ejecutando? Efectivamente se ha constatado que existe evidencia y reporte de situaciones en las cuales se ha puesto en funcionamiento las UPS y que además cuando se detectan fallas por el personal técnico son corregidas.
	¿Los controles son sostenibles? Se ha comprobado en el programa anual de contrataciones que siempre se contemplan los rubros requeridos para el mantenimiento, funcionamiento y actualizaciones de capacidad de respaldos (UPS). Hay garantía en las UPS de los servidores vigentes.

NR	CONTROL A EVAULAR
	C2: El área de Infraestructura tiene configurada y administra un Clúster de Servidores que permite de forma automática intercambiar roles de servidores activo/Pasivo garantizando la disponibilidad del sistema.
	Fuente del Riesgo: Entorno
	Tipo de Riesgo: Riesgo de Activo
	Pruebas Operativas
	Se observó y verificó documentación de planes de contingencia en donde se indica el funcionamiento del Clúster de servidores.
	Se comprobó las configuraciones del Clúster y se revisaron sus logs para validar el funcionamiento.
	Se realizó una prueba controlada con autorización en la cual se constató que a nivel de conectividad los equipos clientes lo que pierden es un 1ms de conexión entre el cambio de roles de servidores.
	Se evidenció en una prueba de sistemas que al momento de intercambio de servidores la transacción que está ejecutándose no se pierdo y concluye satisfactoriamente.
	Pruebas de Diseño
2	**¿Están diseñados correctamente los controles?** El control tiene un diseño correcto ya que se ha podido validar en la configuración del clúster que no existen problemas.
	¿El que ejecuta cada control es el adecuado? El control se ejecuta de forma adecuada por la programación automatizada que realizó el personal de infraestructura de redes.
	¿Se ejecuta cada control en el momento adecuado? El control al momento de una falla en el servidor principal activo se ejecuta cambiando al otro servidor de modo standby a modo activo; asumiendo el rol de los procesos y usuarios de la red.
	¿Hay evidencia que los controles se están ejecutando? Se ha encontrado en los archivos log del clúster evidencias que demuestran que ha habido intercambios de roles de pasivo a activo y de activo a pasivo. Demostrando que si se ejecuta el control.
	¿Los controles son sostenibles? Se ha comprobado que existen planes de mantenimiento para los servidores y el SAN[137] del clúster y además existen rubros en el Programa anual de contrataciones que garantizan los repuestos y accesorios para los componentes del Clúster.

[137] **SAN**: Storage Area Network, español red de área de almacenamiento.

NR	CONTROL A EVAULAR
3	**C3:** El jefe de infraestructura de Red y Base de datos tiene mecanismos de respaldos (Backup cada dos horas) fuera del clúster que son luego copiados a un servidor virtual de Backup para garantizar la disponibilidad de los sistemas al fallar el clúster.
	Fuente del Riesgo: Entorno
	Tipo de Riesgo: Riesgo de Activo
	Pruebas Operativas
	Se han revisado los planes de contingencia con Gerente de TI y Personal de Infraestructura de Redes validando los procedimientos y su efectividad.
	Se verificó la existencia del servidor virtual y se constató que está en línea todo el tiempo.
	Se realizo prueba de los respaldos efectuados al descomprimirlo y adjuntarlos al servidor virtual para probar operatividad de los sistemas.
	Se han revisado los logs de los respaldos y se efectúan conforme a lo programado.
	Pruebas de Diseño
	¿Están diseñados correctamente los controles? El control está bien diseñado pues contiene respaldos independientes del clúster y a la vez independientes del equipo virtual lo cual proporciona una independencia de recursos y redundancia en Backup.
	¿El que ejecuta cada control es el adecuado? El personal que ejecuta es el Jefe de Infraestructura y posee la experticia y autorización requerida para ejecutar el control al momento del incidente. A demás en los planes de contingencia cuenta con personal de Backup en el área de infraestructura capaz de ejecutar la misma tarea.
	¿Se ejecuta cada control en el momento adecuado? Si se ejecuta de forma adecuada ya que al existir una falla en los sistemas el personal de infraestructura tiene monitoreo por WhastupGold indicando el momento en que un recurso está fuera de línea. En ese momento el personal entra en funciones de acuerdo a los planes de contingencia
	¿Hay evidencia que los controles se están ejecutando? Si hay evidencia pues existe un registro de cada uno de los respaldos que se efectúan y se ha podido constatar que el servidor de respaldo virtual está todo el tiempo encendido. A demás se efectúan pruebas semanales de traslado de información de Base de Datos y pruebas de sistemas.
	¿Los controles son sostenibles? El control si es sostenible pues existe planes de pruebas de respaldo y recuperación efectuándose de forma semanal y hay planes anuales de compra de accesorios y repuestos para el servidor real que virtualiza el equipo utilizado para la contingencia.

NR	CONTROL A EVAULAR
4	**C4:** Gerencia de TI por medio del área de infraestructura de redes posee Router, Switches de capa 2 y 3 de respaldos para sustituir equipos dañados.
	Fuente del Riesgo: Entorno
	Tipo de Riesgo: Riesgo de Activo
	Pruebas Operativas
	Se ha comprobado que en la bodega de la Gerencia de TI existen Switches y Routers de Backup.
	Se han verificado los planes de mantenimiento de los equipos de redes.
	Se han comprobado la existencia de respaldos de las configuraciones de todos los equipos de redes.
	Se han verificado el estado de las garantías de los equipos de redes. El resultado es la vigencia de garantías hasta un máximo de 7 años.
	Se tienen planes de cambios de infraestructura de redes cada 8 años para garantizar la disponibilidad de la red.
	Pruebas de Diseño
	¿Están diseñados correctamente los controles? Los controles están bien diseñados pues los equipos de redes que se tienen de respaldos están previamente configurados y se tienen respaldos de las configuraciones de los equipos de producción.
	¿El que ejecuta cada control es el adecuado? El personal de infraestructura de redes que ejecuta este control es calificado con experiencia en Cisco CCNA[138] y redes de computadoras. Se tienen personal suficiente para esta tarea.
	¿Se ejecuta cada control en el momento adecuado? Gerencia de TI posee un sistema de monitoreo de todos los equipos de la red capaz de enviar alertas cuando un equipo falla. Las alertas son enviados al Gerente de TI, Jefe de Infraestructura de Redes y Soporte Técnico de infraestructura.
	¿Hay evidencia que los controles se están ejecutando? Si existen registros en la bitácora del personal de infraestructura en donde se demuestra los momentos que han ocurrido fallas de equipos y como han sido sustituidos. A demás existen planes de contingencia que describen el paso a paso en este tipo de problemas.
	¿Los controles son sostenibles? Los controles si son sostenibles pues existen planes de mantenimiento de los equipos de redes y en el programa anual de contrataciones hay compras programadas de Switches. Otro elemento importante son las Garantías de los equipos vigentes.

[138] **CCNA:** Cisco Certified Network Associate, en español asociado en redes con certificación cisco.

NR	CONTROL A EVAULAR
5	**C5:** El personal de infraestructura administra un IPS que realiza bloqueos proactivos ante ataques a servidores de correos y equipos de red.
	Fuente del Riesgo: Entorno
	Tipo de Riesgo: Riesgo de Activo
	Pruebas Operativas
	Se han validado la existencia de respaldos de configuraciones del UTM que posee la función de IPS.
	Se ha comprobado que existe firma vigente del IPS en el UTM.
	Se ha podido observar el funcionamiento de bloqueo automático de ataques en el IPS y se han revisado historiales de ataques guardados.
	Se comprobaron la existencia de los Logs generados por el IPS.
	Pruebas de Diseño
	¿Están diseñados correctamente los controles? Se ha comprobado que el control está bien diseñado pues el IPS posee las configuraciones necesarias para registrar y bloquear los ataques. A demás sus licencias y firmas están vigentes.
	¿El que ejecuta cada control es el adecuado? Si es adecuado el personal de infraestructura que administra el IPS pues han sido adiestrados por el fabricante y tienen experiencia en IPS como el SNORT.
	¿Se ejecuta cada control en el momento adecuado? En el monitoreo del IPS se observa la existencia de contadores de bloqueos efectuados y además se guardan pantallas de todos los registros de ataques.
	¿Hay evidencia que los controles se están ejecutando? Si existen evidencias de que los controles están activos y que sus reglas están bien configuradas. Hay registros de bloqueo y un servidor de Logs.
	¿Los controles son sostenibles? Se ha comprobado que anualmente se compra la suscripción de las licencias del UTM que contiene al IPS. A demás hay respaldos de las configuraciones y planes de mantenimiento para ese equipo.

NR	CONTROL A EVAULAR
6	**C6:** Soporte Técnico de Infraestructura de Red monitorea por medio de SolarWinds NetWorkMonitor Memoria, CPU y tráfico del Router principal y Switch Core para asegurar funcionamiento correcto bloqueando conexiones extrañas en el tráfico analizado.
	Fuente del Riesgo: Causadas por las personas de forma accidental
	Tipo de Riesgo: Riesgo de Proceso
	Pruebas Operativas
	Se ha comprobado la existencia de la licencia para poder utilizar el software SolarWinds NetworkMonitor
	Se ha comprobado que el software está bien instalado y que opera con normalidad.
	Se tienen respaldos de las configuraciones de los sensores que están siendo monitoreados
	Se ha comprobado que el personal tiene manuales del software y adiestramiento para su utilización.
	El hardware donde está instalado el software tiene su garantía vigente y se cuenta con equipo de respaldo.
	Pruebas de Diseño
	¿Están diseñados correctamente los controles? Si está diseñado bien el control pues el software para el monitoreo es adecuando y se tienen en base a históricos umbrales de niveles adecuados de uso de memoria, procesador e interfaces.
	¿El que ejecuta cada control es el adecuado? El personal de infraestructura de redes que monitorea y realiza bloque en el Router cuando se amerita está capacitado para efectuar dicha actividad y posee registros de actividades realizadas.
	¿Se ejecuta cada control en el momento adecuado? Si se ha comprobado que el control se ejecuta en el momento correcto pues el software de SolarWinds notifica de forma inmediata cuando los umbrales programados son excedidos.
	¿Hay evidencia que los controles se están ejecutando? Si se ha podido comprobar que el control está funcionando al poder ver en funcionamiento el software SolarWinds y revisar los logs generados por los sensores.
	¿Los controles son sostenibles? Si es sostenible el control pues se ha instalado en un equipo con alta capacidad de procesamiento y configuración en RAID 1. A demás la licencia está con mantenimiento de software y se paga anual.

NR	CONTROL A EVAULAR
	C7: El personal de soporte técnico de infraestructura monitorea Tráfico con WireShark para validar los protocolos usados y planifica un Checklist por áreas para validar software instalado y accesos.
	Fuente del Riesgo: Causadas por las personas de formas deliberadas
	Tipo de Riesgo: Riesgo de Proceso
	Pruebas Operativas
	Se ha comprobado en visita al área de infraestructura la existencia de la herramienta WireShark en equipos del personal y con fecha de instalación a acorde a los planes de actualizaciones presentados.
	Se ha encontrado un manual de uso de WireShark y se ha verificado que se tienen manuales operativos desarrollados por personal de infraestructura de GTI.
	Se han revisado los planes de visitas a los usuarios y comprobado los Checklist aplicados.
	Pruebas de Diseño
7	**¿Están diseñados correctamente los controles?** El control está diseñado de forma correcta al poder validar la existencia de manuales de operación en la gestión de incidentes. La forma en que opera es también adecuada ya que los planes de validación son aleatorios y se programan en varios días del mes.
	¿El que ejecuta cada control es el adecuado? El personal de infraestructura es el personal calificado para realizar esta tarea de monitorear y es el que ha creado reglas en WireShark para encontrar cuando se está escaneando puertos o utilizando conexiones SHELL[139] reverso.
	¿Se ejecuta cada control en el momento adecuado? El control se ejecuta durante varios días mensualmente y de forma aleatoria para que los usuarios no esperen cuando realicen las validaciones.
	¿Hay evidencia que los controles se están ejecutando? Si existen registros en los que se han detectado incidencias de escaneo de puertos y han sido detectadas por el WireShark.
	¿Los controles son sostenibles? El control si es sostenible pues hay constantes actualizaciones del WireShark y sus programaciones están respaldadas y son compatibles con las versiones nuevas.

[139] **SHELL**: Termino utilizado para referirse a Interprete de comandos

NR	CONTROL A EVAULAR
8	**C8:** La Gerencia de TI por medio del manual de uso de equipos y medios informáticos está facultada para emitir memorando con sanciones administrativas y cobros por daños a equipos y medios informáticos. **C9:** Personal de Soporte Técnico posee de respaldo Fuentes de Poder, teclado, ratón y periféricos para ser utilizados cuando se requiera.
	Fuente del Riesgo: Causadas por las personas de forma accidental
	Tipo de Riesgo: Riesgo de Activo
	Pruebas Operativas
	Se ha podido obtener copia del manual de uso de equipos y medios informáticos.
	Se ha comprobado que existe un expediente en el que están almacenados los diagnósticos y reportes de cambios efectuados por el personal de Soporte Técnico.
	Se ha comprobado que existen componentes de hardware para equipos y periféricos de clientes en resguardo por el personal de Soporte Técnico.
	Se ha validado con recursos humanos la existencia del listado de personal y las fechas de los programas de concientización.
	Pruebas de Diseño
	¿Están diseñados correctamente los controles? Los controles están diseñados de forma correcta ya que el **C8** es empleado solo cuando el usuario por descuido o agrede daña algún componente de hardware y el **C9** Es implementado cuando por desperfecto de fábrica o por funcionamiento se daña algún dispositivo de hardware. A demás si el usuario lo daña el **C9** también es aplicado.
	¿El que ejecuta cada control es el adecuado? El personal de Soporte Técnico y el Gerente de TI son los responsables de realizar el cambio del hardware y autorizar dichos cambios de forma respectiva.
	¿Se ejecuta cada control en el momento adecuado? Si es ejecutado cada control en el momento adecuado pues cuando se produce un evento que dañe algún componente este es de acuerdo al manual reemplazado y hay registro de esos eventos.
	¿Hay evidencia que los controles se están ejecutando? Si existen evidencias que contienen firmas de los usuarios a los que se les ha reemplazado algún componente de hardware y existe un expediente donde se deja copia de los memos enviados por daños provocados.
	¿Los controles son sostenibles? Los controles son sostenibles ya que existen programas de concientización a todos los usuarios de la empresa y hay hardware de respaldo que se adquiere año con año en base a históricos anteriores.

NR	CONTROL A EVAULAR
	C10: Personal de Soporte Técnico es encargado de validar visor de sucesos y consola de servidor de inventarios para saber qué equipo no está reportando inventario.
	Fuente del Riesgo: Defecto de las aplicaciones, Causadas por las personas de forma accidental.
	Tipo de Riesgo: Riesgo de Activo
	Pruebas Operativas
	Se ha validado la existencia del software de inventarios y se revisaron los Logs para validar su funcionamiento.
	Se ha verificado que existe licencia para uso del software de Inventarios.
	Se han encontrado respaldos de los inventarios de todos los equipos de la red.
	Se ha proporcionado por soporte técnico con autorización del Gerente de TI los manuales de configuración del software de inventario y los manuales operativos.
	Pruebas de Diseño
9	**¿Están diseñados correctamente los controles?** El control está bien diseñado pues posee un software automatizado tipo agente instalado en cada cliente y es vinculado al servidor que recibe los reportes. A demás hay procedimientos programados para comprobar los cambios de inventarios.
	¿El que ejecuta cada control es el adecuado? Por la segregación de funciones y por las capacidades del personal de soporte técnico se valida que son el personal adecuado para monitorear y administrar el hardware de todos los equipos.
	¿Se ejecuta cada control en el momento adecuado? El personal de soporte técnico ha monitorea durante el día que el programa de recopilación de inventarios este ejecutándose de acuerdo a la programación establecida.
	¿Hay evidencia que los controles se están ejecutando? Si hay evidencia de la ejecución del control pues se han comprobado en los logs del sistema que el software de inventarios está trabajando correctamente.
	¿Los controles son sostenibles? Si es sostenible el control porque se cuenta con respaldo de la base de datos de los inventarios, manuales de configuración y manuales de operación.

NR	CONTROL A EVAULAR
10	**C11:** El jefe de soporte técnico monitorea el servidor de antivirus para saber si todos los equipos se están actualizando bien. **C12:** Personal de soporte técnico realiza Checklist periódico en periodos de mantenimiento preventivo.
	Fuente del Riesgo: Defecto de las aplicaciones
	Tipo de Riesgo: Riesgo de Proceso
	Pruebas Operativas
	Se ha recibido por el personal de soporte técnico documentos que comprueban la aplicación del Checklist durante los mantenimientos preventivos.
	Se han validado la existencia de las licencias del servidor de antivirus y cada agente cliente está registrado en la consola.
	Se ha podido verificar la configuración y funcionamiento del servidor de antivirus.
	Se ha procedido a tomar un 15 % de la población registrada de forma aleatoria para validar que tengan el antivirus instalado y actualizado.
	Se ha validado que el equipo del servidor antivirus tenga vigente la garantía. Garantía que caduca en un año.
	Pruebas de Diseño
	¿Están diseñados correctamente los controles? Los controles han sido diseñados correctamente ya que existen controles preventivos y correctivos que se aplican para mantener actualizados los antivirus.
	¿El que ejecuta cada control es el adecuado? Si se ha comprobado que por capacidades y segregación de funciones el personal que ejecuta cada control es el adecuado.
	¿Se ejecuta cada control en el momento adecuado? Cada control es ejecutado de forma independiente. En el caso del **C11** el jefe de soporte técnico en sus tareas diarias mantiene el monitoreo de la consola del servidor de antivirus y los Checklist son realizados en base a los planes del mantenimiento.
	¿Hay evidencia que los controles se están ejecutando? Existen bitácoras por el Jefe de Soporte Técnico en donde registra sus operaciones diarias y hay soportes físicos del personal que realiza los mantenimientos preventivos en donde se registran los datos del Checklist.
	¿Los controles son sostenibles? Los controles son sostenibles porque se cuentan con los procedimientos requeridos y las licencias del software antivirus con vigencia para dos años todavía.

NR	CONTROL A EVAULAR
11	**C13:** El aeropuerto cuenta con un Sistema de Supresión de incendios automatizado que administran los bomberos y monitorea Gerencia de TI. **C14:** El aeropuerto cuenta con un Plan de Emergencias ante desastres naturales o provocados que es dirigido por el Comité de Emergencia encabezado por el Gerente General. **C15:** Personal de Seguridad aeroportuaria monitorea las 24 horas las cámaras de vigilancia. **C16:** El aeropuerto cuenta con una Oficina de Contingencia administrada por recursos humanos.
	Fuente del Riesgo: Del entorno
	Tipo de Riesgo: Riesgo de Activo
	Pruebas Operativas
	Se ha podido constatar la existencia del comité de emergencia.
	Se ha verificado la existencia del Plan de Emergencia y se tienen evidencias de su divulgación a todos los trabajadores y personal que labora para otras empresas dentro de la terminal.
	Se ha comprobado que el personal de Gerencia de TI tiene como miembro del Comité de Emergencia al Gerente de TI que es el que organiza a nivel de tecnología la ejecución del plan.
	Pruebas de Diseño
	¿Están diseñados correctamente los controles? Los controles están diseñados de forma correcta al responder cada responsable en base a su rol y experticia.
	¿El que ejecuta cada control es el adecuado? El personal que ejecuta cada control ha sido capacitado y tiene la suficiente experiencia para poder asumir el rol requerido al momento de una contingencia o desastre.
	¿Se ejecuta cada control en el momento adecuado? Cada control se ejecuta de forma adecuada ya que cuando un incidente es disparado de acuerdo al monitoreo del CCTV y a cada sensor instalado. A demás de las comunicaciones de las personas que están capacitadas para detectar incidentes.
	¿Hay evidencia que los controles se están ejecutando? Si existen evidencias de las actas de las reuniones que efectúa el comité de emergencia, Existe documentaciones de el Plan de Emergencia y pruebas de simulacros realizadas.
	¿Los controles son sostenibles? Los controles son sostenibles pues son parte del entrenamiento que el aeropuerto mantiene recurrente en conjunto con los bomberos, la policía y el ejército.

NR	CONTROL A EVAULAR
12	**C17:** Supervisión de Gerencia de TI en toda actividad de cableado.
	Fuente del Riesgo: Causadas por las personas de forma accidental
	Tipo de Riesgo: Riesgo de Proceso
	Pruebas Operativas
	Se ha verificado la existencia del manual de políticas y uso de equipos informáticos en el cual según aprobación por junta directiva brinda al Gerente de TI la autoridad para permitir o no la realización de cableados estructurados.
	Se ha proporcionado por el Gerente de TI copias de algunas de las solicitudes recibidas y todo el plan de trabajo para su ejecución.
	Se ha verificado que en la bitácora del área de infraestructura existe una correlación con las solicitudes aprobadas por el Gerente de TI.
	Pruebas de Diseño
	¿Están diseñados correctamente los controles? Si está diseñado de forma adecuada el control pues según el manual de políticas y uso de equipos informáticos Gerencia de TI debe supervisar y autorizar toda actividad de cableado.
	¿El que ejecuta cada control es el adecuado? El personal que ejecuta esta supervisión por Gerencia de TI es el de infraestructura de redes y posee el conocimiento y experiencia para supervisar todo tipo de cableado estructurado tanto en Fibra Óptica como UTP.
	¿Se ejecuta cada control en el momento adecuado? Si se ejecuta de forma adecuada ya que todo cableado es realizado bajo autorización de la Gerencia de TI y bajo previo estudio.
	¿Hay evidencia que los controles se están ejecutando? Si se tiene evidencia por medio de las solicitudes de servicio que son autorizadas por el Gerente de TI y supervisadas por personal de infraestructura de red.
	¿Los controles son sostenibles? El control es sostenible puesto que existen procedimientos bien definidos y documentaciones que autoriza al Gerente de TI asumir el rol de autoridad aprobatoria de todo trabajo.

7.5. SELECCIÓN DE SOFTWARE SIEM.

Para poder seleccionar el software SIEM adecuado para la organización se ha realizado investigación de las funcionalidades de distintos software SIEM brindados en el cuadrante Mágico de Gartner. Cabe mencionar que existe una amplia lista de proveedores de software SIEM en el mercado y que existe bastante información de cada producto. Si buscamos en internet cualquier software SIEM que este ranqueado en el Cuadrante Mágico de Gartner es fácil de encontrar la documentación provista por Gartner de los comparativos, ventajas y desventajas de cada producto. De acuerdo a las características y a la disponibilidad de pruebas de software en la Web se han seleccionado los siguientes: **Splunk** y **AlienVault (USM[140]/OSSIM[141])**. Estos productos son ofrecidos en modo de prueba hasta por un máximo de 2 meses. Esto permitirá observar el comportamiento del hardware virtual o físico.

Lo primero que se lleva a cabo por un buen periodo de tiempo es la implementación parcial y en modo demo del software SIEM Splunk Enterprise. Ver **Anexo A-1** proceso de instalación de Splunk. Este software Splunk ofrece una licencia de pruebas por un periodo de 2 meses. Para poder evaluar la funcionalidad y viabilidad económica de la utilización de este software se realizan varias instalaciones en periodos de tiempos diferentes. Los resultados de estas pruebas nos brindan el dato estimado de la cantidad de LOG generados por día de los dispositivos de red. Ver **Anexo A-3** volúmenes de LOG generados por principales equipos de la red.

El primer software que se probó fue el Splunk Enterprise. Este software es de fácil instalación y no es con una complejidad relativa para administrar. Ofrece una buena gama de posibilidades para las búsquedas, alertas, reportes y cuadros de mando (Dashboards). En el **Anexo A-2** se muestra el proceso de incorporación de fuentes de datos al software SIEM tanto equipos de red como servidores. El proceso de agregar estos equipos es bastante intuitivo y las búsquedas ofrecen grandes capacidades para generar nuestra propia estructura de datos a consultar ya que se pueden realizar extracciones de datos sobre las cueles se crean reglas más específicas. Ver **Anexo A-4** donde se muestran ejemplo de alertas y búsquedas con Splunk. Con este software se pasaron varios meses de pruebas en los cuales se observó el amplio volumen de LOG generados por los servidores, Router y UTM. Este estudio de muestra de alguno de los principales elementos de la red nos da indicadores que demuestran el consumo promedio de más de 1 GB de 2 equipos de red. Si multiplicamos esto por más de 20 equipos de comunicación y varios servidores el resultado es bastante grande. La primera opción que se probó que es Splunk en su sitio web ofrece cálculo de los pagos a realizar.

[140] **USM**: Unified Security Management, en español Gestión de seguridad unificada.
[141] **OSSIM**: Open Source Security Information Management, en español Sistema de Gestión de la información de seguridad de código abierto.

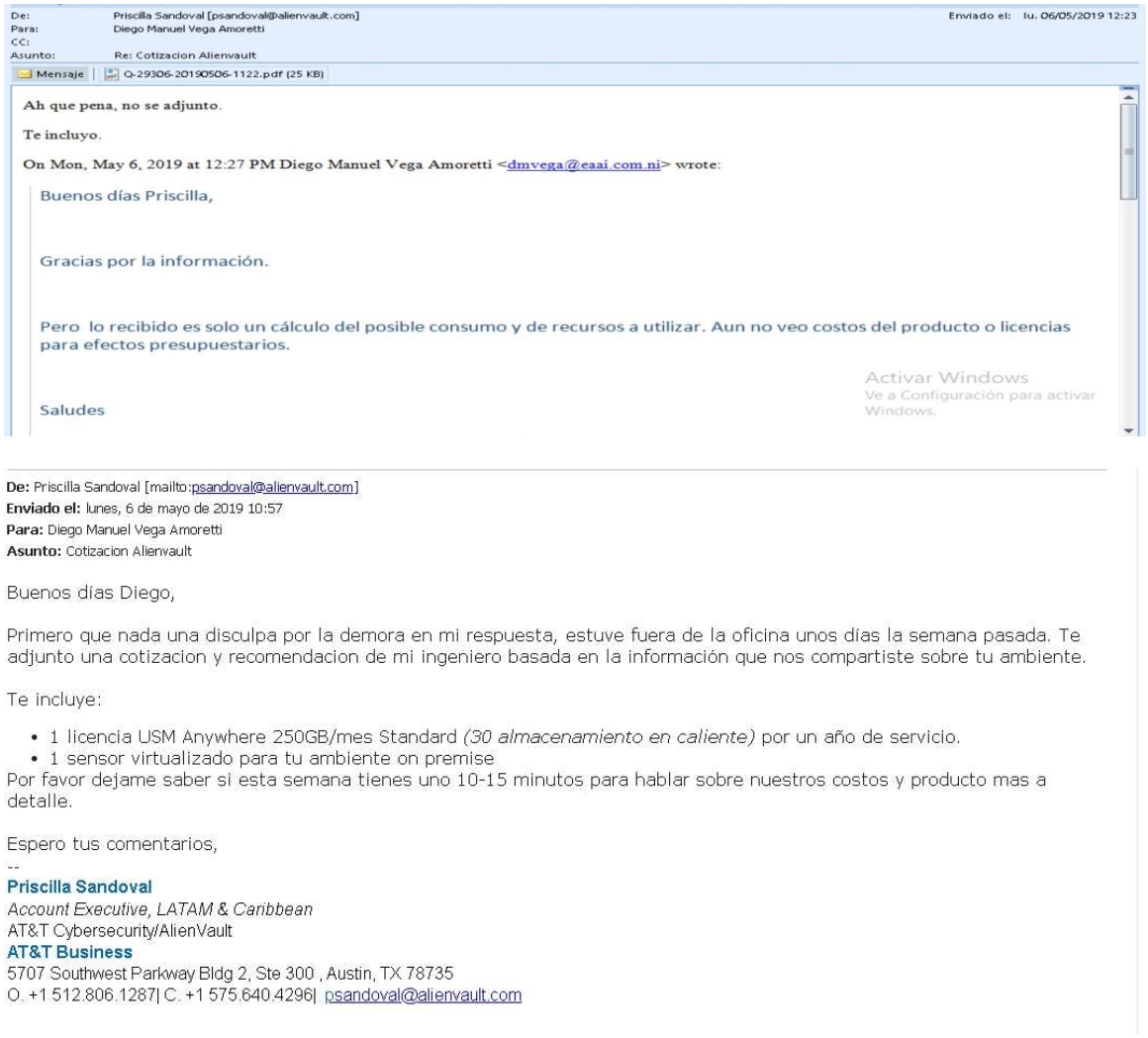
En la **Tabla 7** se muestra un comparativo entre los dos productos, resultando más atractivo el **AlienVault OSSIM** por ser código abierto, gratuito y con muchos beneficios inmediatos.

Tabla 7 Comparativo entre SPLUNK y OSSIM

SPLUNK	ALIEN VAULT OSSIM / USM
Los costos económicos son de los más altos en el mercado. Los clientes de Gartner que han implementado Splunk constantemente generan inquietudes sobre el modelo de licencia y el costo general para implementar la solución. 1 año de licencia con un volumen de 1 GB tiene un costo aproximado de U$ 172,800. Según (Pricing, 2019).	A nivel económico es una solución de bajo costo. Si se usa la USM pagarán una anualidad promedio de 20,000 dólares. Si se usa OSSIM no hay costo asociado a nivel externo.
La plataforma de inteligencia de seguridad de Splunk está compuesta por Splunk Enterprise y dos soluciones premium, Enterprise Security (ES) y Splunk User Behavior Analytics (UBA). Estos poseen capacidades específicas de monitoreo de seguridad, incluidas consultas, visualizaciones y cuadros de mando específicos de seguridad preempaquetados, así como funciones de administración de casos, flujo de trabajo y respuesta a incidentes y analíticas avanzadas	USM Appliance y USM Anywhere ofrecen varias capacidades de seguridad integradas, que incluyen detección de activos, FIM, evaluación de vulnerabilidad y sistemas de detección de intrusos basados en host y en red
Splunk no ofrece una versión del dispositivo de la solución. Las organizaciones que desean una versión del dispositivo en las instalaciones deben trabajar con un socio de Splunk que proporcione la integración en el hardware soportado	Alien Vault OSSIM / USM están disponibles tanto en solución de dispositivo como en la nube. Permite instalación hibrida con un dispositivo local (maquina virtual) y un sensor en la nube.
Configuración con cierto grado de dificultad y administración no muy intuitiva.	Configuración amigable y administración sencilla e intuitiva para usuarios sin mucha experiencia.
Informes muy elaborados y con capacidad de crear los propios.	AlienVault proporciona actualizaciones de contenido a través de sus suscripciones de Threat Intelligence, así como inteligencia de origen de la comunidad, que están integradas en las funciones de monitoreo, detección e informes de USM Appliance y USM Anywhere
(Splunk, 2019) Informa que a partir del 1 de noviembre de 2019, todos los productos y servicios de Splunk contarán con licencias a plazo. Ya no venderán ningún producto con licencias perpetuas.	El tipo de licencia en caso de OSSIM es perpetua y de código abierto. USM tiene el modelo por suscripción mensual, anual, etc.

En el caso de AlienVault USM se realizó un acercamiento a la empresa para obtener datos de los costos de una implementación, ver **Figura No15** Proceso de cotización, de este SIEM para la EAAI. El resultado es el siguiente:

Se recibió correo de **Priscilla Sandoval** que es la ejecutiva de cuentas de AlienVault para Latinoamérica y el Caribe con el precio de una solución SIEM de USM AnyWhere



De: Priscilla Sandoval [psandoval@alienvault.com] Enviado el: lu. 06/05/2019 12:23
Para: Diego Manuel Vega Amoretti
CC:
Asunto: Re: Cotizacion Alienvault
Mensaje | Q-29306-20190506-1122.pdf (25 KB)

Ah que pena, no se adjunto.

Te incluyo.

On Mon, May 6, 2019 at 12:27 PM Diego Manuel Vega Amoretti <dmvega@eaai.com.ni> wrote:

Buenos días Priscilla,

Gracias por la información.

Pero lo recibido es solo un cálculo del posible consumo y de recursos a utilizar. Aun no veo costos del producto o licencias para efectos presupuestarios.

Activar Windows
Ve a Configuración para activar Windows.

Saludes

De: Priscilla Sandoval [mailto:psandoval@alienvault.com]
Enviado el: lunes, 6 de mayo de 2019 10:57
Para: Diego Manuel Vega Amoretti
Asunto: Cotizacion Alienvault

Buenos días Diego,

Primero que nada una disculpa por la demora en mi respuesta, estuve fuera de la oficina unos días la semana pasada. Te adjunto una cotizacion y recomendacion de mi ingeniero basada en la información que nos compartiste sobre tu ambiente.

Te incluye:

- 1 licencia USM Anywhere 250GB/mes Standard *(30 almacenamiento en caliente)* por un año de servicio.
- 1 sensor virtualizado para tu ambiente on premise

Por favor dejame saber si esta semana tienes uno 10-15 minutos para hablar sobre nuestros costos y producto mas a detalle.

Espero tus comentarios,
--
Priscilla Sandoval
Account Executive, LATAM & Caribbean
AT&T Cybersecurity/AlienVault
AT&T Business
5707 Southwest Parkway Bldg 2, Ste 300 , Austin, TX 78735
O. +1 512.806.1287| C. +1 575.640.4296| psandoval@alienvault.com

Figura No 15. Proceso de cotización. (Captura de pantalla de equipo personal)

La información obtenida de precios es la siguiente:

ALIEN VAULT

SALES ORDER FORM - USM ANYWHERE™

Created Date:	5/6/2019	Quote Number:	Q-29306
Quote Expiration Date:	6/28/2019		

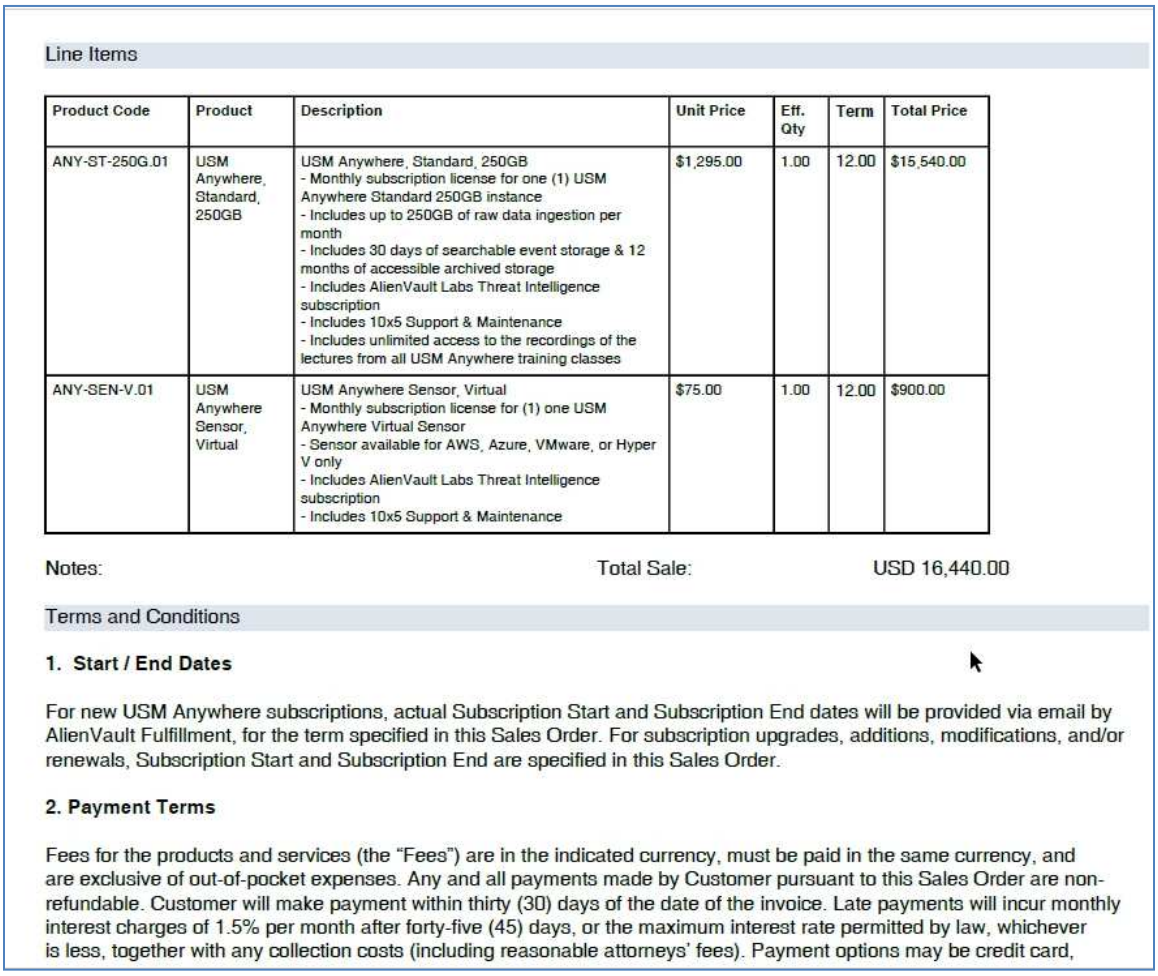
Contact Information

Customer:		**Sales Representative:**	
Account Name:	EMPRESA ADMINISTRADORA DE AEROPUERTOS INTERNACIONALES (EAAI)	Prepared By:	Priscilla Sandoval
Partner:		Email:	psandoval@alienvault.com
Contact Name:	DIEGO VEGA		
Phone:	22331624	**Company Address**	
Email:	dmvega@eaai.com.ni	AlienVault, Inc ("AlienVault")	
Fax:		1100 Park Place, Suite 300	
		San Mateo, CA, USA 94403	
		+1 650 713-3333 (voice)	
		+1 650 212-7637 (fax)	

Address Information

Bill To Name:	EMPRESA ADMINISTRADORA DE AEROPUERTOS INTERNACIONALES (EAAI)	Ship To Name:	EMPRESA ADMINISTRADORA DE AEROPUERTOS INTERNACIONALES (EAAI)
Bill To:	**P.O. BOX 5179** **Km 11 Carretera Norte** **Managua, NI 01001** **Nicaragua**	Ship To:	**P.O. BOX 5179** **Km 11 Carretera Norte** **Managua, NI 01001** **Nicaragua**
Phone:	22331624		
Customer ID:	AV1904-097168		

Figura No 16. Página No1 cotización ALIENVAULT USM (Captura de pantalla de equipo personal)



Line Items

Product Code	Product	Description	Unit Price	Eff. Qty	Term	Total Price
ANY-ST-250G.01	USM Anywhere, Standard, 250GB	USM Anywhere, Standard, 250GB - Monthly subscription license for one (1) USM Anywhere Standard 250GB instance - Includes up to 250GB of raw data ingestion per month - Includes 30 days of searchable event storage & 12 months of accessible archived storage - Includes AlienVault Labs Threat Intelligence subscription - Includes 10x5 Support & Maintenance - Includes unlimited access to the recordings of the lectures from all USM Anywhere training classes	$1,295.00	1.00	12.00	$15,540.00
ANY-SEN-V.01	USM Anywhere Sensor, Virtual	USM Anywhere Sensor, Virtual - Monthly subscription license for (1) one USM Anywhere Virtual Sensor - Sensor available for AWS, Azure, VMware, or Hyper V only - Includes AlienVault Labs Threat Intelligence subscription - Includes 10x5 Support & Maintenance	$75.00	1.00	12.00	$900.00

Notes: Total Sale: USD 16,440.00

Terms and Conditions

1. Start / End Dates

For new USM Anywhere subscriptions, actual Subscription Start and Subscription End dates will be provided via email by AlienVault Fulfillment, for the term specified in this Sales Order. For subscription upgrades, additions, modifications, and/or renewals, Subscription Start and Subscription End are specified in this Sales Order.

2. Payment Terms

Fees for the products and services (the "Fees") are in the indicated currency, must be paid in the same currency, and are exclusive of out-of-pocket expenses. Any and all payments made by Customer pursuant to this Sales Order are non-refundable. Customer will make payment within thirty (30) days of the date of the invoice. Late payments will incur monthly interest charges of 1.5% per month after forty-five (45) days, or the maximum interest rate permitted by law, whichever is less, together with any collection costs (including reasonable attorneys' fees). Payment options may be credit card,

Figura No 17. Página No2 cotización ALIENVAULT USM (Captura de pantalla de equipo personal)

Estos datos obtenidos en las **Figura No16** y **Figura No17** fueron en base a el ánalisis de los equipos a conectar en el SIEM. Para este efecto se llenó un formulario y se envió un correo a Priscilla Sandoval. Ver **Anexo A-5** Formulario para Precio AlienVautl.

7.6. CARACTERÍSTICAS Y REQUISITOS DE HARDWARE DEL SIEM

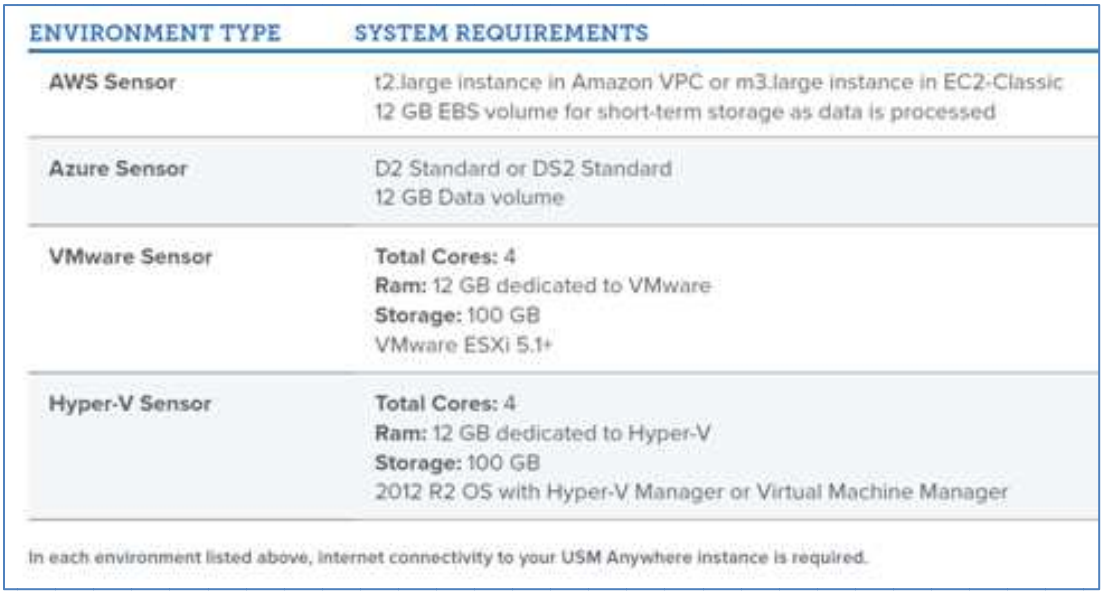
Para la implementación de cualquier software SIEM en la empresa es necesario tener en cuenta características robustas en el hardware del equipo que llevará a cabo las labores almacenamiento de un gran volumen de LOGS, capacidades de alto procesamiento y altas capacidades de manejo de memoria RAM. Para este efecto y pensando en un volumen de datos de 45 Gb por mes se pretende proponer el siguiente hardware:

La **Tabla 8** muestra la tabla de características técnicas requeridas para un equipo SIEM según (Splunk, Installation Manual, 2019) .

Tabla 8. Requerimientos de Hardware de Splunk

Plataforma	Hardware y Configuración Recomendada
No Windows	2 Procesadores de 6 cores, 2+ GHz, RAM 12GB, RAID 1, Sistema Operativo de 64 Bit
Plataformas Windows	2 Procesadores de 6 cores, 2+ GHz, RAM 12GB, RAID 1, Sistema Operativo de 64 Bit

Se ha obtenido vía correo las especificaciones para el servidor AlienVautl, ver en la siguiente página la **Figura No.18**. Requerimientos AlienVault.



ENVIRONMENT TYPE	SYSTEM REQUIREMENTS
AWS Sensor	t2.large instance in Amazon VPC or m3.large instance in EC2-Classic 12 GB EBS volume for short-term storage as data is processed
Azure Sensor	D2 Standard or DS2 Standard 12 GB Data volume
VMware Sensor	**Total Cores:** 4 **Ram:** 12 GB dedicated to VMware **Storage:** 100 GB VMware ESXi 5.1+
Hyper-V Sensor	**Total Cores:** 4 **Ram:** 12 GB dedicated to Hyper-V **Storage:** 100 GB 2012 R2 OS with Hyper-V Manager or Virtual Machine Manager

In each environment listed above, internet connectivity to your USM Anywhere instance is required.

Figura No 18.Requerimientos AlienVautl. (Captura de información recibida por representante de AlienVautl Priscilla Sandoval)

Tabla de características técnicas de equipo rsyslog

El equipo previo al SIEM que se encargará de almacenar los LOG de los servidores de correos y DNS puede ser un equipo físico o virtual. Los requisitos mínimos para que este sea funcional se muestran en la **Tabla 9**.

Tabla 9.Requerimientos LOG Server.

DESCRIPCIÓN	CARACTERÍSTICA
Sistema Operativo	Centos 7 o superior Red Hat Enterprise 7.2 o superior
Procesadores	Procesadores Intel Core i7 2.4 GHZ (8 Cores) Procesadores Intel Xeon 2.4 GHZ (12 Cores)
Memoria	De 8 a 12 GB RAM
Almacenamiento	Raid 1 con volumen de 1 a 2 TB
Tipo de Arquitectura	64 Bit.

Estos equipos pueden ser físicos o virtuales. Por lo que se ha validado la infraestructura de la empresa y se ha determinado la existencia de un Cluster de VWARE con capacidades altas de procesamiento, memoria, almacenamiento y con una SAN de varios Teras. Por ende se proponen virtualizar los equipos mencionados.

7.7. ARQUITECTURA DEL SIEM A UTILIZAR

En base a la decisión costo beneficio de utilizar **OSSIM** (Open Source Security Information Management System, en español Sistema de gestión de la información de seguridad Open Source) definiéremos de forma general su arquitectura. Pero antes podemos decir que OSSIM fue desarrollado con propósito de gestionar la información de seguridad de una red. Esta plataforma integran más de 22 productos de seguridad todos ellos "Open Source" (en español código abierto). Estos productos integrados son utilizados por OSSIM para correlacionar. Las soluciones de código libre de seguridad para la monitorización y detección que incluye OSSIM entre otras son: snort, nessus, ntop, nmap y nagios; estas son integradas en una arquitectura abierta que se aprovechará de todas sus capacidades para aumentar la seguridad de las red.

La arquitectura que compone OSSIM ha venido a crear un Framework (Marco de Trabajo) capaz de recolectar toda la información de los diferentes Plugins (en español complementos o componentes externos de código abierto) con propósito de integrar e interrelacionar entre sí para obtener una visualización única del estado de la red (Generando Visibilidad en la Infraestructura). Todas las bondades de este SIEM producen la capacidad de detección de anomalías, priorizar los eventos según el contexto en el que se producen y mejorar la visibilidad de la monitorización del estado de la red actual.

Según (Análisis de la plataforma Ossim, 2008) por **Puchades Olmos, Adrian** como muchos otros dicen que OSSIM se divide en tres capas:

- Capa Inferior
- Capa Intermedia
- Capa Superior

A continuación se describen cada una.

- **Preprocesado (Nivel Bajo o Capa Inferior):** Se conoce como la capa o nivel más bajo; consiste en todos los denominados detectores, monitores o preprocesadores que forman parte de la red y que realizan funciones de detección y generación de alertas. Dicho de otras palabras son todos los componentes claves que producen algún tipo de información o que monitorean otros activos de la red y que luego envían información a un dispositivo de almacenamiento de LOG y correlación. Dentro de estos elementos están:

    1. Sistemas de Detección y Prevención de Intrusos (UTM, HIDS, NDIS): snort, sophos, watchguard, etc.
    2. Detectores de anomalías.
    3. Cortafuegos o Firewall, Firewall de Aplicaciones (Windows Aplication Firewall): Denominado F5
    4. Varios tipos de Monitores: Software especializado como SolarWinds o PRTG.

- **Postprocesado (Nivel Intermedio):** En el nivel intermedio se realiza el postprocesado donde OSSIM realiza una abstracción de eventos incompresibles y luego se convierten en alarmas comprensibles: este proceso se lleva a cabo principalmente en el motor de correlación y está siendo accedido o modificado por las directivas de correlación que permiten unir diferentes eventos de bajo nivel en una única alarma de alto nivel aumentando la sensibilidad y la fiabilidad de la red. Las tareas efectuadas son:

    1. Normalización.
    2. Correlación.
    3. Priorización.
    4. Valoración de Riesgos.

- **Front-End (Nivel Alto):** El “Front-end” o interfaz de usuario final es la herramienta de gestión que permite configurar y visualizar tanto los módulos externos como los propios del Framework. Mediante esta interfaz podremos crear la topología de la red, inventariar activos, crear las políticas de seguridad, definir las reglas de correlación y enlazar las diferentes herramientas integradas. Es en si la capa que muestra los resultados de los eventos correlacionados y permite al usuario final administrar o definir sus propias alarmas.

De acuerdo a lo anterior expuesto ver el diagrama de capas de OSSIM en la **Figura No.19**. Capas OSSIM

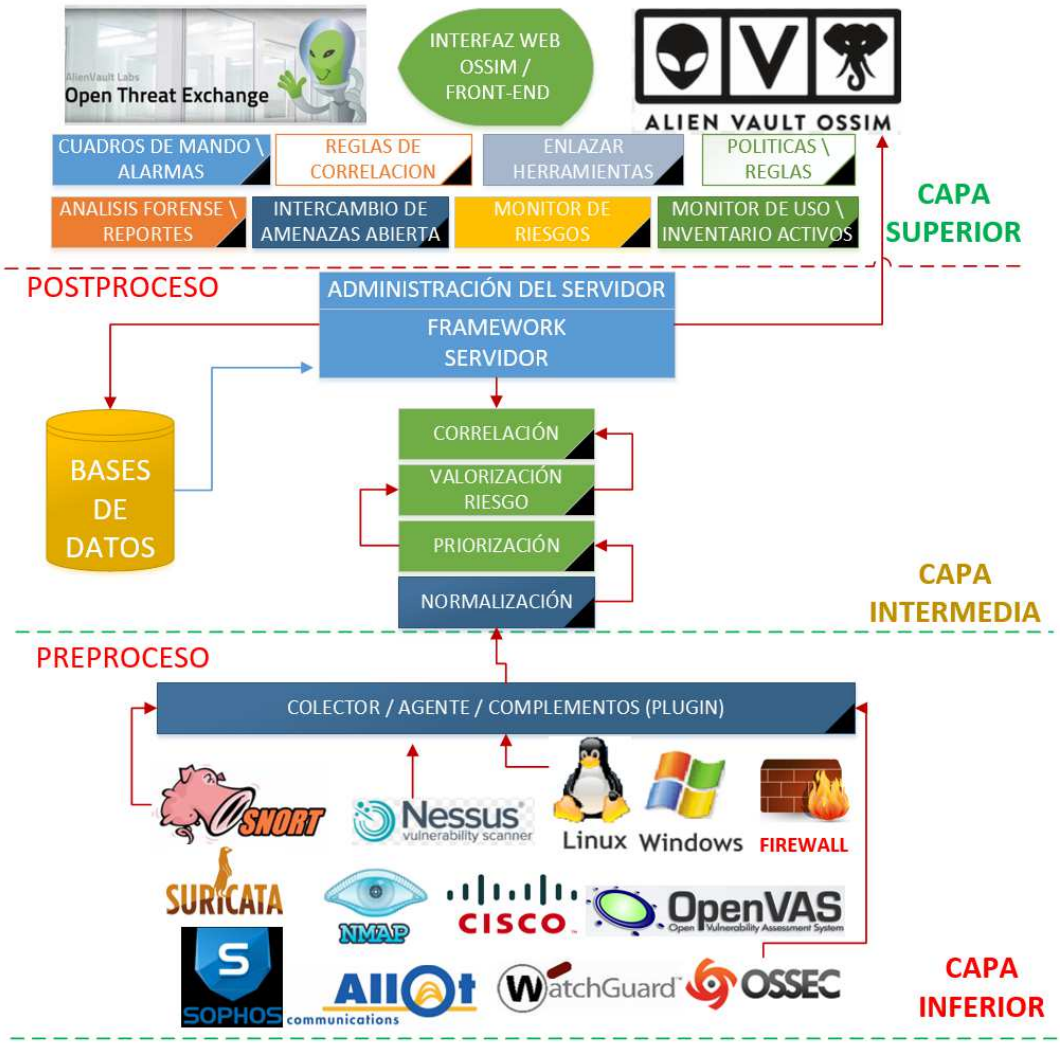


Figura No 19. Capas OSSIM. (Desarrollo Propio)

Luego de conocer las capas en que se divide OSSIM podemos definir que la arquitectura su arquitectura se divide en dos partes. Una es realizada por una arquitectura distribuida basa en agentes, sensores, detectores o monitores que forman parte del preproceso de OSSIM. La otra parte es la centralizada que está basada en todo el marco de trabajo que trae integrado el servidor, que es en donde se centralizan los procesos después de la recolección. Proceso que son denominados postprocesos. En este caso podemos ver según la **Figura No.20** Arquitectura de OSSIM toda la relación que existe desde el momento que un LOG o Agente ingresa datos para ser normalizados para luego caer a una cadena de

procesos que inicia con la priorización, valoración y luego son correlacionados.

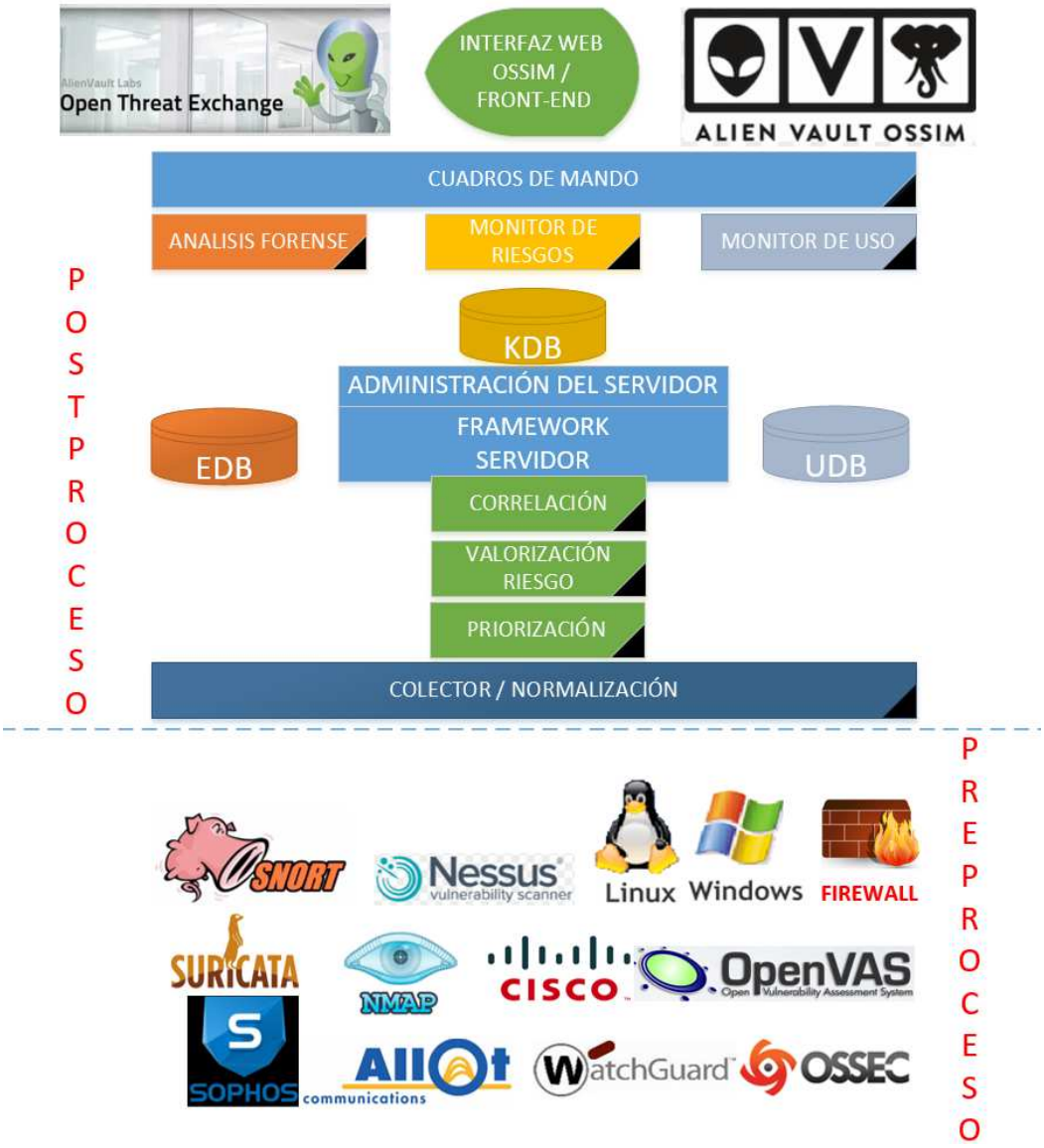


Figura No 20. Arquitectura de OSSIM (Desarrollo Propio)

Las tres bases de datos heterogéneas para los distintos tipos de datos almacenados que utiliza la arquitectura de OSSIM en la **Figura No 20**. Tienen la siguiente función o utilidad:

- **EDB:** Es la base de datos de eventos, muy probable siempre la más voluminosa pues almacena todos los eventos recibidos desde los detectores, agentes o monitores.

- **KDB:** Es la base de datos del Framework (en español marco de trabajo), en ella se almacena toda la información referente a la red y la definición de la política de seguridad.

- **UDB:** Es la base de datos de perfiles, esta almacena todos los datos aprendidos por el monitor de perfiles.

Dentro de las herramientas que forman parte del marco de trabajo (FrameWork) de OSSIM se encuentran:

- **Arpwatch:** Utilizado para la detección de nuevos equipos conectados en la red.
- **P0f:** Análisis pasivo para la detección y análisis de sistemas operativos conectados en la red. OpenVas: Escaneo de vulnerabilidades para infraestructura y aplicaciones web.
- **Snort:** Detector de intrusos en red.
- **OSSEC:** Agente que valida la integridad de archivos, instalación de programas no autorizados, creación de usuarios locales o cambios en sistema operativo.
- **MySQL:** Base de datos para el almacenamiento de todos los eventos registrados manteniéndolos disponibles para ser consultados posteriormente.

Durante el proceso de normalización de eventos OSSIM utiliza una serie de campos producto de la normalización. Estos campos son obtenidos de distintas fuentes de datos pero al aplicar la normalización OSSIM detecta cada campo si está presente en el LOG. Ver Anexo **A-6 Campos Normalizados de OSSIM**.

7.8. FUNCIONALIDAD DEL SIEM A IMPLEMENTAR

Para describir la funcionalidad el SIEM haremos uso del modelo de tres capas de OSSIM e iniciaremos a explicar el contenido. La imagen de la **Figura No 21**. Funcionalidad de OSSIM nos describe el orden de abajo arriba de como las capas se relacionan.

Figura No 21. Funcionalidad de OSSIM. (Desarrollo Propio)

La funcionalidad de OSSIM describiendo desde su capa de preproceso que es donde los sensores o agentes envían la información al servidor hasta la capa de Front-End (Interfaz de Usuario Final) inicia con los Detectores de Patrones(1) que son las aplicaciones (HIDS[142], NIDS[143], IPS, IDS, Firewall) capaces de escuchar tráfico en la red en busca de patrones malignos por medio de reglas que son definidas en sus firmas. Lo más común que estos dispositivos usan son expresiones regulares o reglas con sintaxis propias en cadenas de texto. En este sentido OSSIM posee integrado varios tipos de detectores de patrones dentro de los cuales está Snort, snare y Osiris. El elemento que acompaña a los detectores de patrones en la capa de preproceso son los Detectores de Anomalías(2), estos son más inteligentes que los anteriores puesto que no se

[142]**HIDS**: *Host-based intrusion detection system , en español Sistema de detección de intrusos en un Host. .*
[143]**NDIS**: *Network Intrusion Detection System, en español Sistema de detección de intrusos en una Red*

basan en reglas sino en el aprendizaje de comportamientos fuera de lo común; ya que estos son capaces de aprender los comportamientos habituales y decidir de forma automatizadas cuales son correctos y cuáles no. Un ejemplo claro del empleo de un detector de anomalías es el cambio de una dirección IP o MAC. En el caso de OSSIM Detectores de anomalías incluidas son:

- ***Spade:*** Detecta conexiones no usuales por puertos y destinos utilizados. Usado para mejorar el reconocimiento sobre ataques sin firma.
- ***Aberrant Behaviour***: Plugin (Complemento) para **Ntop** aprende el uso de parámetros y alerta cuando dichos parámetros se salen de los valores esperados.
- ***ArpWatch:*** utilizado para detectar cambios de mac.
- ***Pof***: utilizado para detección de cambios de sistema operativo.
- ***Pads y Nmap:*** Utilizado para detectar anomalías en los servicios de red.

La siguiente capa de funcionalidad de OSSIM es el postproceso en la que la Normalización(3) es el primer paso de esa capa. En esta etapa no solo se colectan los LOG de todos los dispositivos sino que se lleva a cabo la normalización de estos, que es el proceso de unificar todos los LOG en un mismo formato y única consola. Pero para esto el OSSIM posee un parser (en español traductor) que es capaz de conocer todos los formatos de los dispositivos que se integran al OSSIM y que luego que los homogeniza se encarga de almacenarlos en una base de datos llamada "**EDB**" (Event Database, en español base de datos de eventos). Esta base de datos es la más voluminosa. De tal forma que una vez homogenizados los datos de acuerdo a los campos requeridos por OSSIM y mencionados en el **Anexo A-6**, este permitirá la detección de patrones más complejos.

Luego de la normalización sigue la etapa de Priorización(4) que se basa en una serie de políticas definidas que permiten establecer la prioridad de los eventos que están ocurriendo. Pero esto se define en base a la alimentación que se da en el contexto de la información asignada a todos los recursos activos de la topología de red. En el caso de OSSIM se almacena en una base de datos

llamada "**KBD**" (Knowledge Database, en español base de datos de conocimiento). Lo que se almacena son los datos de los equipos (inventarios de activos y redes) y políticas de acceso. A través de la valoración de alertas se realizará una de las partes más importantes del filtrado de alertas recibidas por los detectores. Desde el framework (en español marco de trabajo) del sistema podremos configurar las siguientes características:

- Política de Seguridad
- Inventario de las maquinas de la red.
- Valoración de activos.
- Valoración de amenazas.
- Valoración de fiabilidad de cada alerta.
- Definición de alarmas.

Para que el proceso de priorización sea efectivo se debe realizar una continua y detallada especificación de la situación de la organización.

Con una base de conocimientos de la información bien alimentada el otro elemento importante es la Valorización de riesgos. Para esto OSSIM realiza sus cálculos del valor de riesgo. Estos cálculos toman en cuenta los siguientes tres factores:

- El valor del activo "equipo" implicado sobre el evento.
- La amenaza que representa el evento o cuánto daño puede hacer al activo implicado.
- La probabilidad de que este evento ocurra.

Por lo general en las empresas existe una valoración tradicional del riesgo, en el caso de OSSIM el riesgo lo calcula en tiempo real. En este caso el valor del riesgo se medirá como el daño que produciría el evento y la probabilidad de que esté ocurriendo en este momento la amenaza. Está probabilidad, derivada de la imperfección de los detectores (falsos positivos), y representará el grado de

fiabilidad de estos en la detección de una posible intrusión. Por ello, el valor de riesgo instantáneo producido por la recepción de una alerta, dependerá del daño que produciría el ataque, la probabilidad de que este ocurra y la fiabilidad que el detector proporciona. Según (Event Details Fields, 2019) a fórmula que OSSIM emplea para el cálculo del riesgo es la siguiente:

Riesgo = Valor del activo * Confiabilidad del evento * Prioridad del evento / 25

En esta fórmula, el valor del activo es un valor de 0 a 5; este debe ser asignado por su organización. La prioridad del evento es una clasificación de prioridad de 0 a 5 que se basa en el tipo de evento. Un tipo de evento tal como: falla de autenticación, ataque web o denegación de servicio. Esto indica la urgencia con que un evento debe ser investigado. (AlienVault proporciona una taxonomía de eventos para clasificar varios eventos por categoría y subcategoría. La fiabilidad (se compara con la efectividad de un control) del evento es un clasificación de confiabilidad de 0 a 10 que especifica la probabilidad de que un evento sea un ataque real o un falso positivo evento.

OSSIM posee un Monitor de Riesgos que valora el riesgo acumulado en el tiempo sobre las redes y grupos de trabajo relacionados con un evento.

Un factor clave dentro de la funcionalidad de OSSIM es la Correlación(6). Este motor de correlación podemos definirlo como un algoritmo que realiza operaciones por medio de datos de entradas para ofrecer un dato de salida (una alarma o alerta, la ejecución de una actividad). El motor de correlación desarrollado en OSSIM, se encarga de comprobar cada uno de los eventos recibidos y busca evidencias o síntomas que prueben la veracidad de un ataque o si se trata de un falso positivo.

OSSIM ha desarrollado un modelo de correlación que tiene la capacidad de:

- Desarrollar patrones específicos para detectar lo conocido y detectable.

- Desarrollar patrones ambiguos para detectar lo desconocido y no detectable.
- Poseer una máquina de inferencia configurable a través de reglas relacionadas entre sí capaz de describir patrones más complejos.
- Permitir enlazar Detectores y Monitores de forma recursiva para crear cada vez objetos más abstractos y capaces.
- Desarrollar algoritmos que ofrezcan una visión general de la situación de seguridad de la red.

Este motor se alimenta de los monitores (indicadores de estados) y detectores (alertas). De tal forma que la salida del motor de correlación puede ser una alerta o un indicador.

El proceso de correlación se rige mediante tres métodos heterogéneos pero con un mismo objetivo, estos son:

- **Correlación mediante secuencia de eventos (Correlación lógica):** Se centra en buscar ataques conocidos y detectables, relaciona a través de reglas que implementarán una máquina de estados, los patrones y comportamientos conocidos que definen un ataque. La base principal son los arboles de decisión como los utilizados en inteligencia artificial. Una características importante es que el motor de correlación de OSSIM acepta fuentes hibridas (monitores y detectores), se pueden definir orígenes, su arquitectura es recursiva, se pueden definir prioridad y fiabilidad en las alertas y su estructura jerárquica permite correlación en topología distribuida.

- **Correlación mediante algoritmos Heurísticos:** Este método detectará situaciones sin conocer patrones y comportamientos que definen un ataque. Implementa funciones que mediante funciones heurísticas intentará descubrir situaciones de riesgo que se alejan del comportamiento cotidiano, intentará suplir la incapacidad del método

anterior, además se podrá obtener una visión general del estado de seguridad de la red. La base principal de este modelo de correlación es la acumulación de eventos en el tiempo. El algoritmo que se usa es denominado CALM(Compromiso and Attack Level Monitor, en español compromiso y monitor de nivel de ataque)

- **Correlación mediante inventariado:** Los ataques recibidos tienen siempre como objetivo un determinado "sistema operativo, servicio especifico, etc..". Con el inventario de la red podremos descartar falsos positivos a maquinas que no cumplen dichas características y priorizar las maquinas de mayor riesgo como los servidores. Para este modelo se realiza un inventario automático en los sensores con detectores pasivos que permiten de forma pasiva ver el tráfico de la red. También se realiza de forma centralizada desde el servidor, mediante analizadores de red que de forma activa encuentran hosts y servicios.

Una vez que se tienen los eventos correlacionados finalizamos la etapa del postprocesado de eventos. Ahora estamos a nivel de Front-End (Interfaz de usuario final) y uno de los elementos indispensables es el uso de Monitores(7). OSSIM realiza varios tipos de monitorización, estos son:

- **Monitor de Riesgos (RiskMeter):** Proporciona los valores producidos por el algoritmo CALM (usado en correlación heurística), valores que miden el nivel de riesgo de compromiso "C" y el de ataque "A" procedentes de la recepción de alertas que indican que una determinada maquina ha sido comprometida o está siendo atacada.
- **Monitor de Uso**: Provee los datos generales del tráfico de la máquina, como el número de bytes que transmite al día.

- **Monitor de Perfiles**: Brinda los datos específicos del uso realizado por el usuario y permite establecer un perfil, (por ejemplo el uso de correo smtp, pop3 y http, en perfil de usuario normal); estos datos se obtienen de la base de datos de perfiles "**UDB**" (User Database, en español base de datos de usuario).
- **Monitor de Sesión**: Permite ver en tiempo real las sesiones que están activas por los usuarios. Ofrece una foto instantánea de la actividad de una maquina en la red.
- **Monitor de Caminos**: Genera en tiempo real una representación de los caminos o rutas trazados en la red por diferentes máquinas que interactúan entre ellas en un intervalo de tiempo. Este monitor obtiene sus datos de dos de los monitores descritos anteriormente. Estos son: El Monitor de sesiones que proporciona cada uno de los enlaces del momento y el Monitor de Riesgo que proporciona el nivel de riesgo de cada máquina para representar cada camino con un color diferente y calcular el riesgo agregado. El proceso de monitorización se puede realizar únicamente mostrando las sesiones tcp o brindando tanto udp como tcp. Incluir un icmp puede implicar un mapa de red enredado.
- **Monitor de Disponibilidad**: La información de disponibilidad es importante para detectar ataques de denegación de servicios. OSSIM incluye el plugin (Complemento en español) "Nagios" capaz de chequear y mostrar la disponibilidad o no de servicios y equipos en la red.
- **Monitorización Personalizada**: Existe un plugin (Complemento en español) parametrizable que permite crear monitores personalizados, que extraen cualquier parámetro que se quiera recopilar, filtrar y enviar al motor de correlación para ser procesado.

Al igual que los Monitores también existe en esta capa de alto nivel la denominada Consola Forense(8). Esta consola es un frontal Web que permite la consulta a toda la información almacenada en el colector. Esta consola es un buscador que ataca a la "**EDB**" (Event Database, en español base de datos de

eventos) y permite al administrador analizar a posteriori y de una forma centralizada los eventos de seguridad de todos los elementos críticos de la red. A diferencia del monitor de riesgos esta consola permite profundizar al máximo detalle sobre cada uno de los eventos ocurridos en el sistema.

La última funcionalidad de OSSIM a nivel del Front-End (en español interfaz de usuario final) son los Cuadros de Mando(9). En estos cuadros es donde se podrá configurar una visión a alto nivel del estado de seguridad de la red. Cada cuadro de mando monitorizará una serie de indicadores definidos que medirán el estado de seguridad de la organización. A demás se definen los umbrales que debe cumplir la organización. Podemos decir en rasgos generales que son la principal herramienta para saber en todo momento que ocurre en la red; puesto que están mostrando la información más concisa y simple posible. A través de él se enlazara con cada una de las herramientas de monitorización para profundizar en cualquier elemento que deseemos o que constituya un llamado de atención para nosotros.

8. IMPLEMENTACIÓN DE SIEM

8.1. DEFINICIÓN DE ALCANCE DE SIEM

El software SIEM a implementar puede en dependencia de la economía de la empresa utilizar licencia para todos los equipos. Pero en la realidad la situación económica y el costo de cada software SIEM no permitirían sostener un proyecto de este tipo. Por consiguiente se debe asegurar que la lista de equipos críticos obtenidos en el análisis de controles críticos nos brinde los elementos básicos asegurados. En este efecto se debe seleccionar como mínimo:

1. Router Cisco nodo principal.
2. Administrador de Ancho de banda Allot NetEnforcer.
3. UTM Watchguard.
4. Router de cada terminal aérea.
5. Switches de Terminal Managua
6. Servidores de Aplicaciones y base de datos.
7. Servidores de Correos y DNS
8. Servidor de Antivirus

Para efectos de este proyecto no se llevará a cabo la implementación completa del SIEM, lo que se realizará es un demo de algunos equipos de la LAN y se utilizará una versión de software con licencia temporal o características limitadas. El presente trabajo dejará las bases para la implementación futura del software SIEM que permitirá la implementación de un SOC (Security Operación Center, en español Centro de Operaciones de Seguridad). Ver **Anexo A-8** Proceso de Aprobación de Piloto SIEM

8.2. DEFINICIÓN DE POLÍTICAS

Desde el punto de vista interno la empresa y la Gerencia de TI están regidas por las siguientes leyes, decretos o normativas para todos los procesos y servicios a nivel tecnológico.

- Manual de Control Interno de la EAAI.
- Código de Conducta de la EAAI.
- Manual de Equipos y Medios Informáticos
- Plan de Contingencia.

Dichos códigos, manuales y planes están enfocados a disminuir los riesgos, y controlar la operación de los diferentes sistemas/información que maneja la EAAI

Existen programas de seguridad para concientizar a los usuarios contenidas en el plan de capacitación anual a todo el personal, de igual manera existen procedimientos de entrenamientos y capacitaciones en los que los usuarios están involucrados directamente sobre todo en las pruebas contenidas en el plan de contingencia con el fin de lograr una mejora continua y reducir los riesgos antes las posibles amenazas a los procesos y servicios existente en la EAAI.

En el Manual de equipos y Medios informáticos se tienen establecidas los roles y responsabilidades de los usuarios, así como los procedimientos adecuados para el uso de este en el cumplimento de las políticas de seguridad establecidas y aprobadas por la Dirección Ejecutiva.

Para la correcta implementación de un software SIEM la empresa debe garantizar como mínimo el cumplimiento de las siguientes políticas de seguridad y operatividad en el área de Infraestructura de Redes.

Políticas del Área de Infraestructura de Redes.

- Actualizaciones periódicas de los sistemas operativos de los equipos.
- Monitoreo constantes de todos los recursos de infraestructura.
- Uso de Port-Security.
- Implementación de VLANs
- Amarre de Mac e IP.
- Los puertos no registrados en la base de datos de administración de redes deben estar apagados.
- Configurar ACLs a nivel de cada equipo de comunicación (Switches o Routers) para permitir a ciertos equipos los accesos.
- Realizar respaldos de las configuraciones de cada equipo.
- Realizar monitoreo de trafico de red, uso de memoria y procesador de los equipos de red.
- Monitorear cada puerto de los Switches el consumo de ancho de banda con el uso herramientas de software como el PRTG Network Monitor que se posee bajo licencia para 1000 sensores.
- Mantener actualizado el mapeo de la red por medio de software como LAN Surveyor
- Mantener el inventario de activos de infraestructura actualizados.

Políticas implementadas a Nivel de Servicios.

- Validar la disponibilidad de los recursos de hardware que proporcionan soporte al software SIEM y Syslog a implementar.
- Implementar controles adicionales al SIEM que gestionen logs
- Mantener filtrados los puertos permitiendo que solo estén abiertos los que son de utilidad para los servicios y aplicativos.
- Limitar en los correos los tipos de archivos admitidos bloqueando los que suelen ser nocivos.
- Bloquear los puertos o servicios no autorizados.

8.3. CONFIGURACIONES PREVIAS A SENSORES

Los Sensores a integrar en el SIEM son los equipos de red como Switches y Router por medio de la configuración de un syslog. En el caso de la empresa se tienen Switches Cisco y Dell. Para el caso de los equipos Cisco sólo se debe activar el envío de log y configurar algunos parámetros básicos. La **Figura No.22** y **Figura No 23** muestran los comandos a Ejecutar en Cisco.

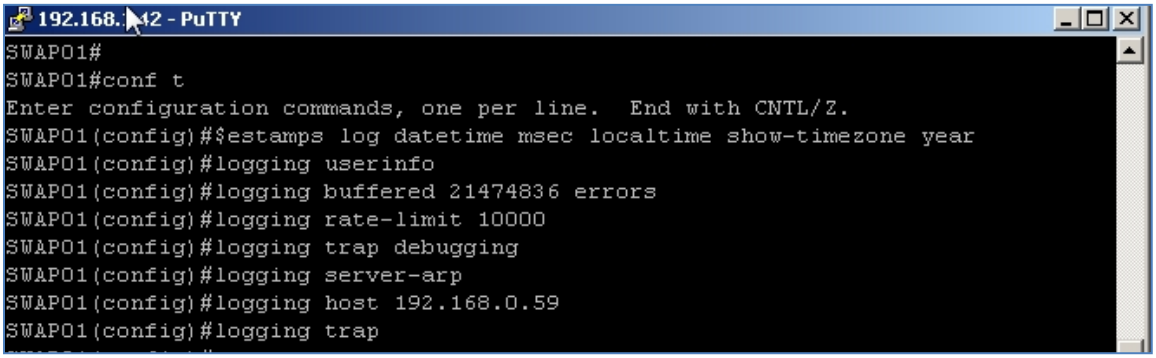


Figura No 22. Configuración Switch Cisco (Captura de pantalla de equipo personal)**.**

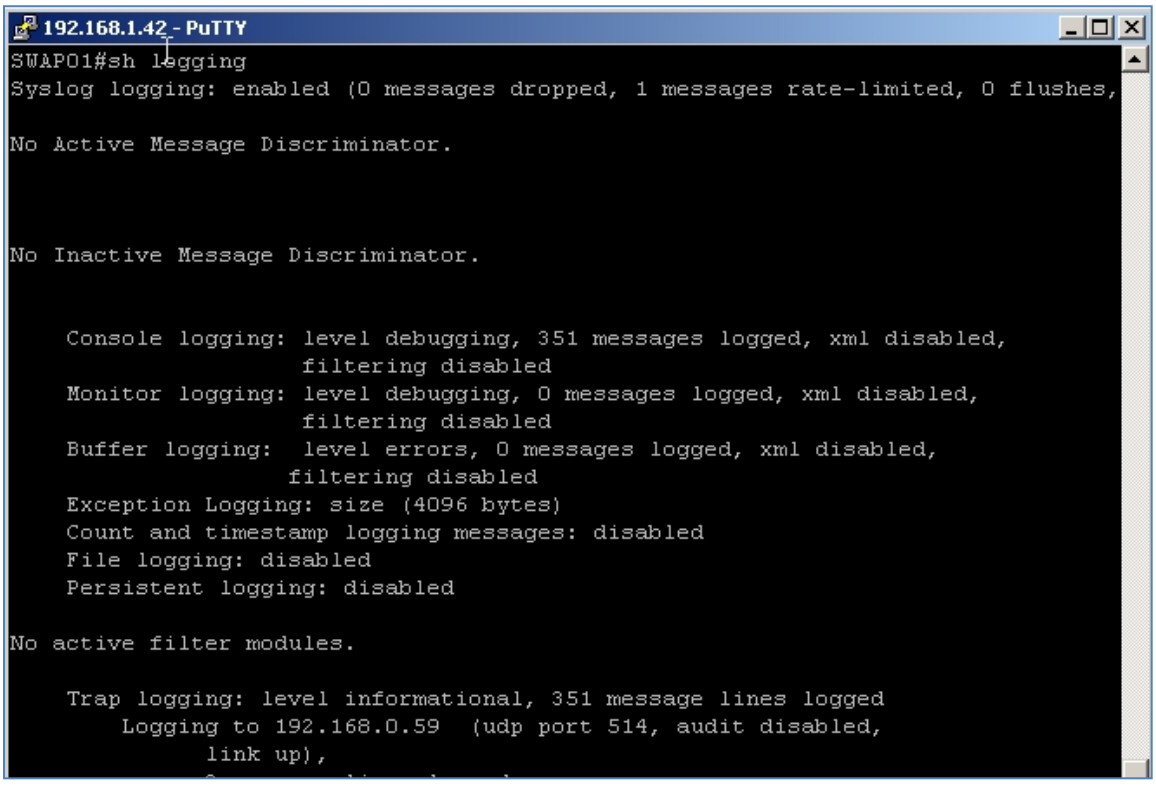


Figura No 23. Configuración Switch Cisco Completada (Captura de pantalla de equipo personal)**.**

En el caso de los equipos DELL se puede hacer vía comando o vía gráfica. Primero se habilita lo que se desea enviar de log tal como se observa en la **Figura No 24**.

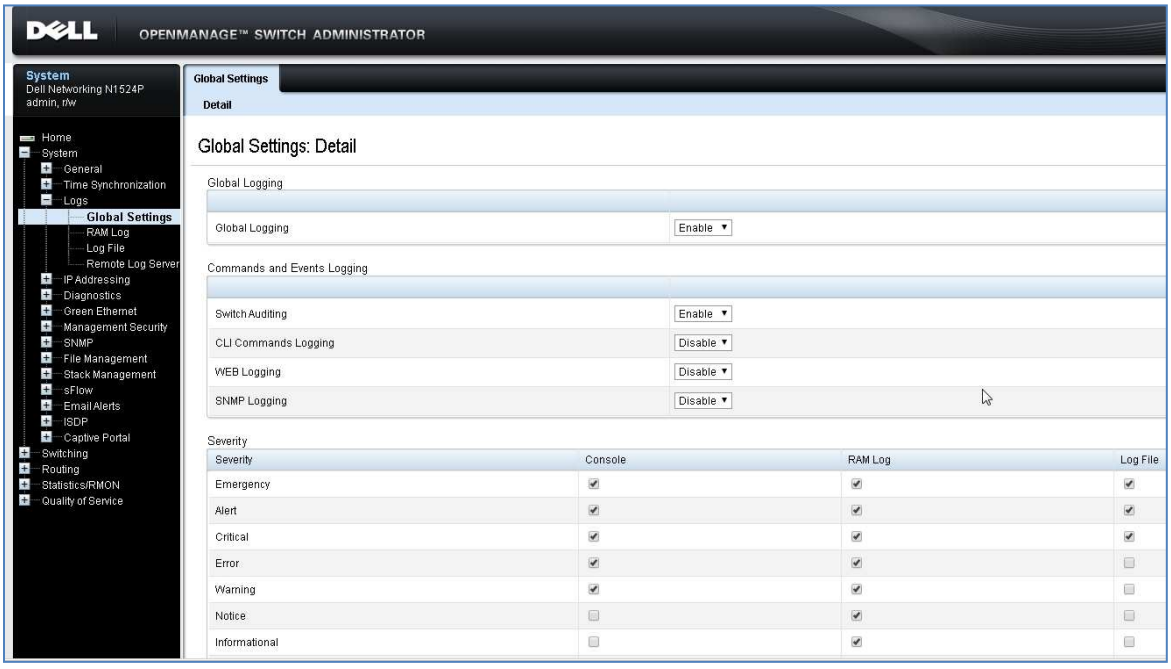


Figura No 24. Configuración Switch DELL Web (Captura de pantalla de equipo personal)

Luego de establecer la configuración global debemos ir al menú del Switch en la opción "Remote Log Server" se hace clic en "Add" (Agregar), luego se llenan los campos "Log Server" (Se escribe el IP), "UDP Port" (Se escribe el puerto UDP 514), se escribe en "Description" (Para que será utilizado) y se Marcan los tipos de Log a enviar en "Severity". Ver todas las opciones que en la **Figura No 25** se habilitaron.

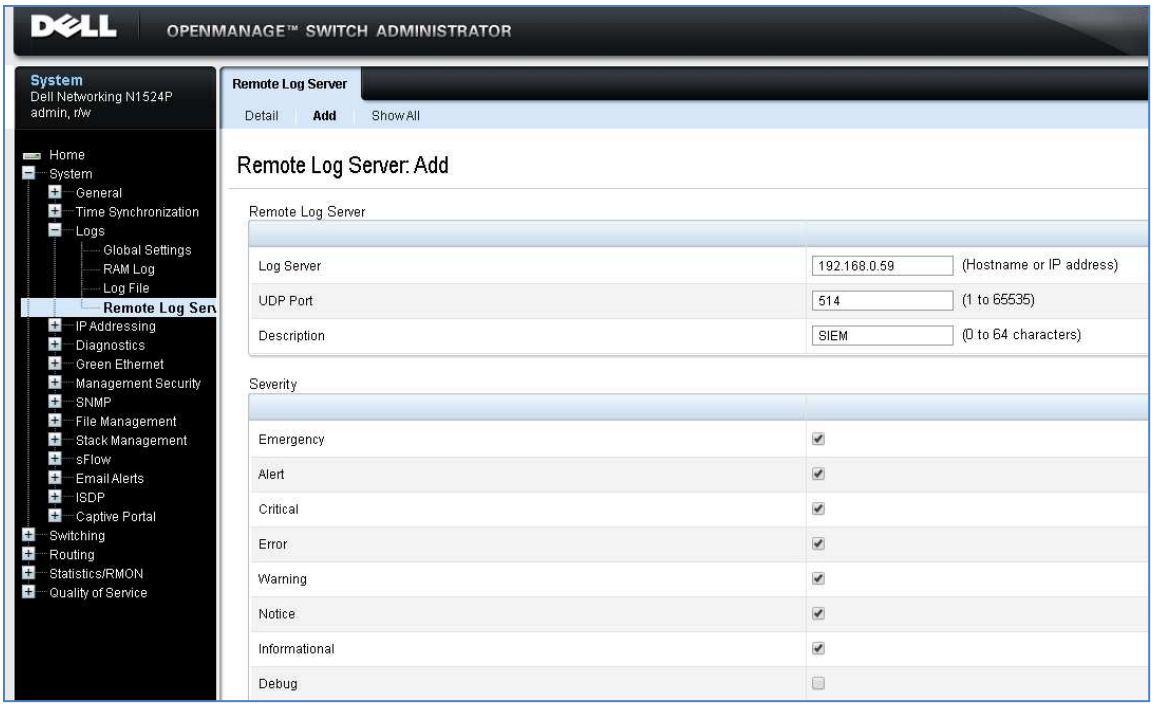


Figura No 25. Campos de LOG seleccionados en Switch DELL (Captura de pantalla de equipo personal)

El envío de LOG para nuestro SIEM ha sido configurado, ver **Figura No 26**.

Figura No 26. Servidor Remoto activo en Switch DELL (Captura de pantalla de equipo personal)

En la **Figura No 27** se muestra el caso del UTM WatchGuard, para este equipo solo se configura en la opción "Servidor de syslog" el IP del equipo remoto, el IP del SIEM, luego el puerto que es el 514 y se establece el tipo de formato como syslog.

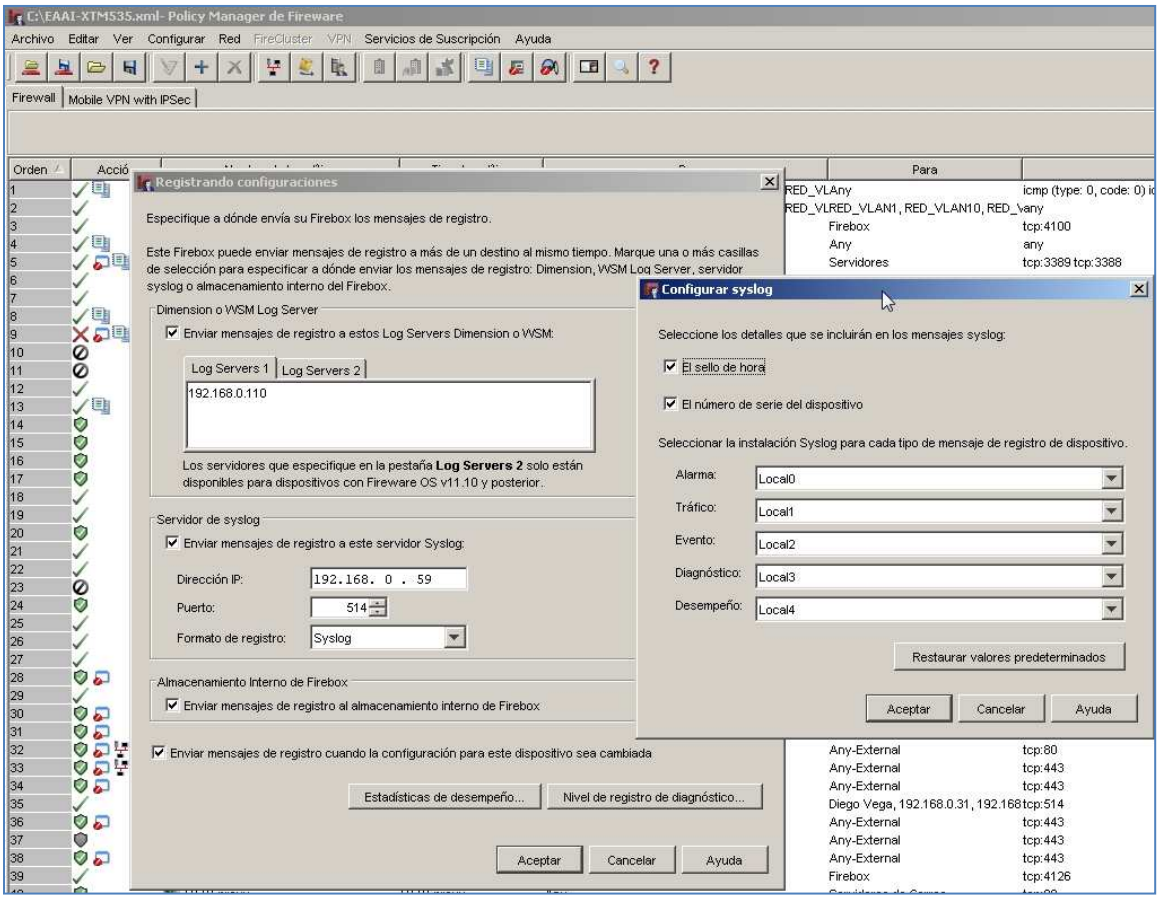


Figura No 27. Configuración de Syslog en UTM (Captura de pantalla de equipo personal)

Para los Servidores Linux o Windows solo se debe asegurar al momento de instalar los agentes que enviaran los log que el firewall no les bloquee.

8.4. INSTALACIÓN Y CONFIGURACIÓN DE SIEM

El proceso de instalación del SIEM inicia con la elección de la plataforma de hardware sobre al cual se montará el software. En este caso se ha definido de acuerdo a las posibilidades de la empresa el uso de equipos virtuales, ver **Figura No 28**. Por lo tanto se provisionara de dos equipos virtuales. Un equipo para el Syslog Server y un equipo para el Software SIEM. A continuación se muestra la configuración de la máquina virtual del equipo LogServer.

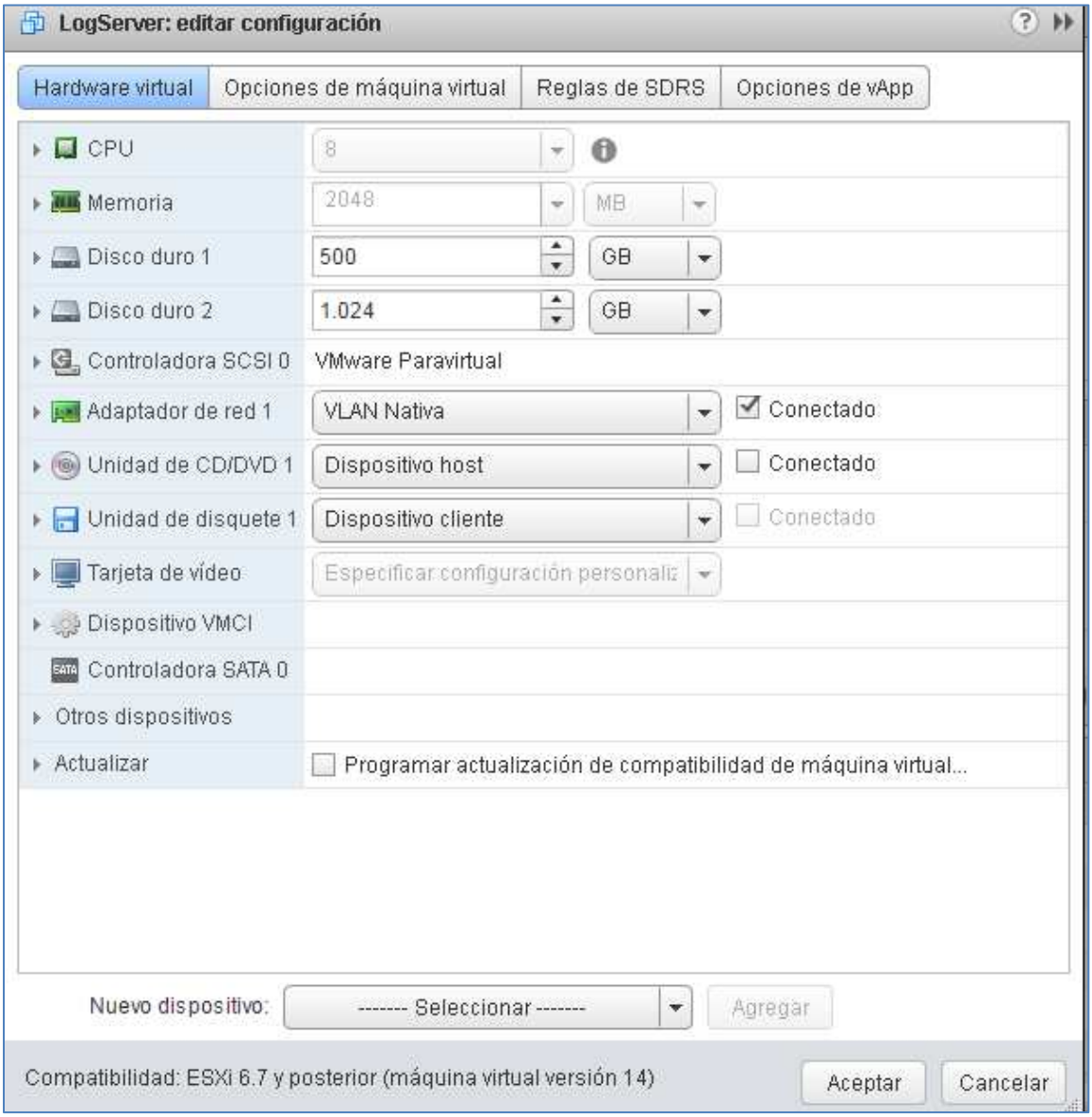


Figura No 28. Maquina Virtual para LOG Server (Captura de pantalla de equipo personal)

Como se observa el requerimiento es menor al mínimo en un ambiente de producción. Pero el equipo cómo se gestiona vía comandos es 100% funcional.

En el Anexo **A-7 Configuración de LOG Server** se muestra el proceso de creación de servidor de LOG. En ese apartado se muestra como se configura rsyslog para recibir log de equipos remotos incluyendo UTM o cualquier PC.

El software SIEM a utilizar por tema de costos en la versión gratuita de AlienVault llamado OSSIM. La **Figura No 29** muestra la configuración del equipo virtual para OSSIM.

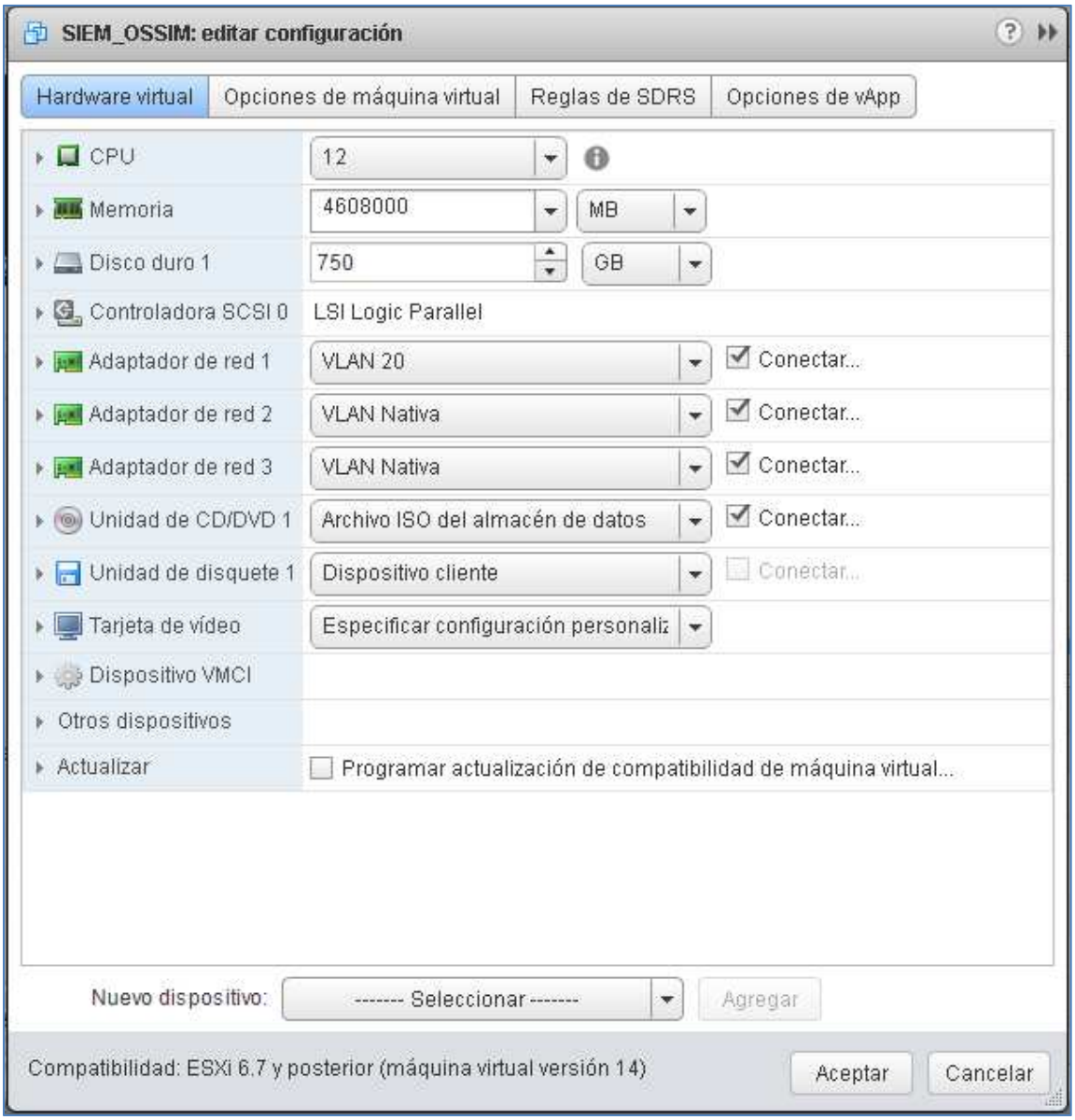


Figura No 29. Maquina Virtual para OSSIM (Captura de pantalla de equipo personal)

Como se observa en la **Figura No 29** el aprovisionamiento seleccionado en memoria es mínimo. La cantidad de cores es la recomendada. La capacidad de disco es pequeña por el hecho de que la implementación no será de toda la

infraestructura. Se utilizaran pocos equipos. Se utilizaran 3 tarjetas de red (Gestión, integración de equipos y búsquedas).

A partir de este momento se describe el proceso de instalación de AlienVault. Se ha descargado la imagen ISO oficial del sitio y se ha integrado al equipo virtual para su instalación. Como se observa la **Figura No 30** este instalador pesa 736 MB. La versión es de 64 Bits.

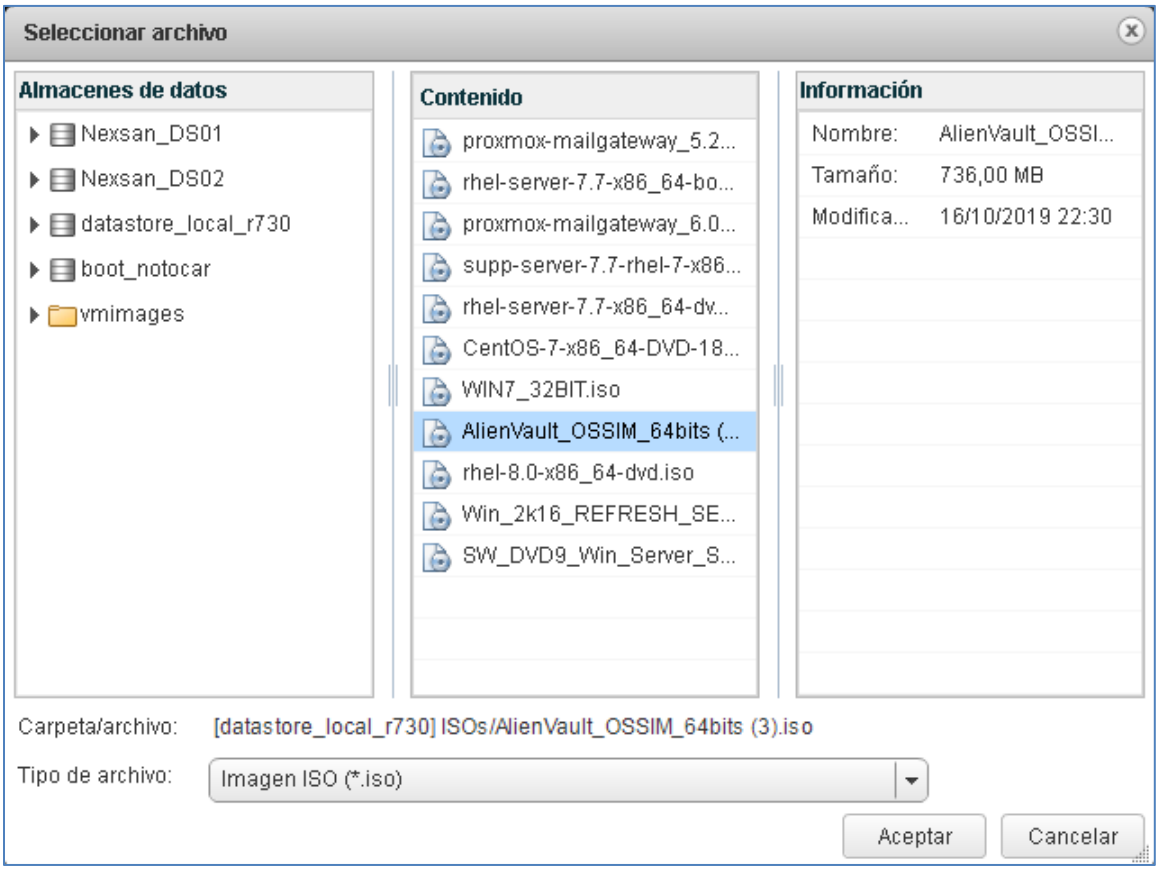


Figura No 30. Selección de ISO OSSIM (Captura de pantalla de equipo personal)

Con la imagen ya cargada en el equipo virtual inicia el proceso de instalación.

La primera pantalla de OSSIM permite seleccionar si lo que se desea es instalar AlienVault Sensor o AlienVault OSSIM. En nuestro caso seleccionamos OSSIM. Tal como se muestra en la **Figura No 31**.

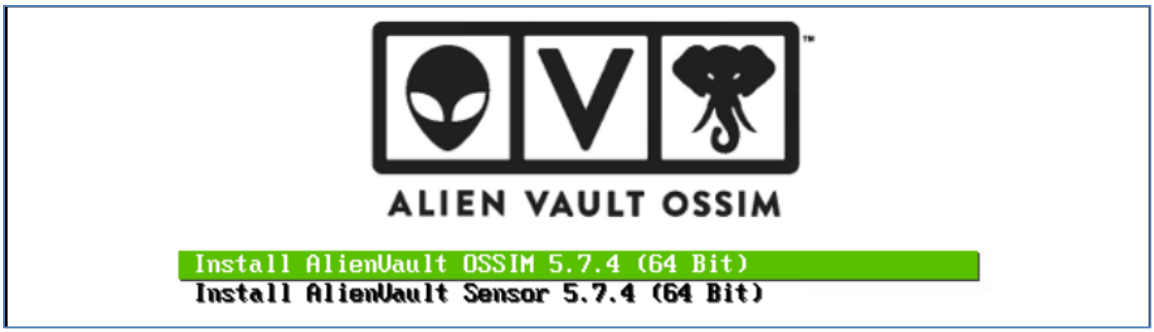


Figura No 31. Selección de OSSIM en Instalador (Captura de pantalla de equipo personal)

La **Figura No 32** del instalador consiste en seleccionar el idioma que utilizaremos durante todo el proceso de instalación.

Figura No 32. Selección de idioma (Captura de pantalla de equipo personal)

Lo que ahora nos toca realizar con el idioma ya actualizado en español es establecer el país en donde se está instalando el SIEM OSSIM. Esta información es importante porque los usuarios que hace uso de la versión gratuita de OSSIM se suscriben al sitio web y tienen acceso a varios recursos que incluye los denominados pulsos que consisten en los reportes efectuados por todos los usuarios de OSSIM en el mundo. De tal forma que si algún evento de seguridad, ataques masivos, se llevan a cabo en Nicaragua nosotros por nuestra ubicación seremos alertados. De igual forma la herramienta gráfica proporciona un cuadro de mando o DashBoard que ubica en el mundo todos los eventos de seguridad generados. Ver **Figura No 33**. (Captura de pantalla de equipo personal)

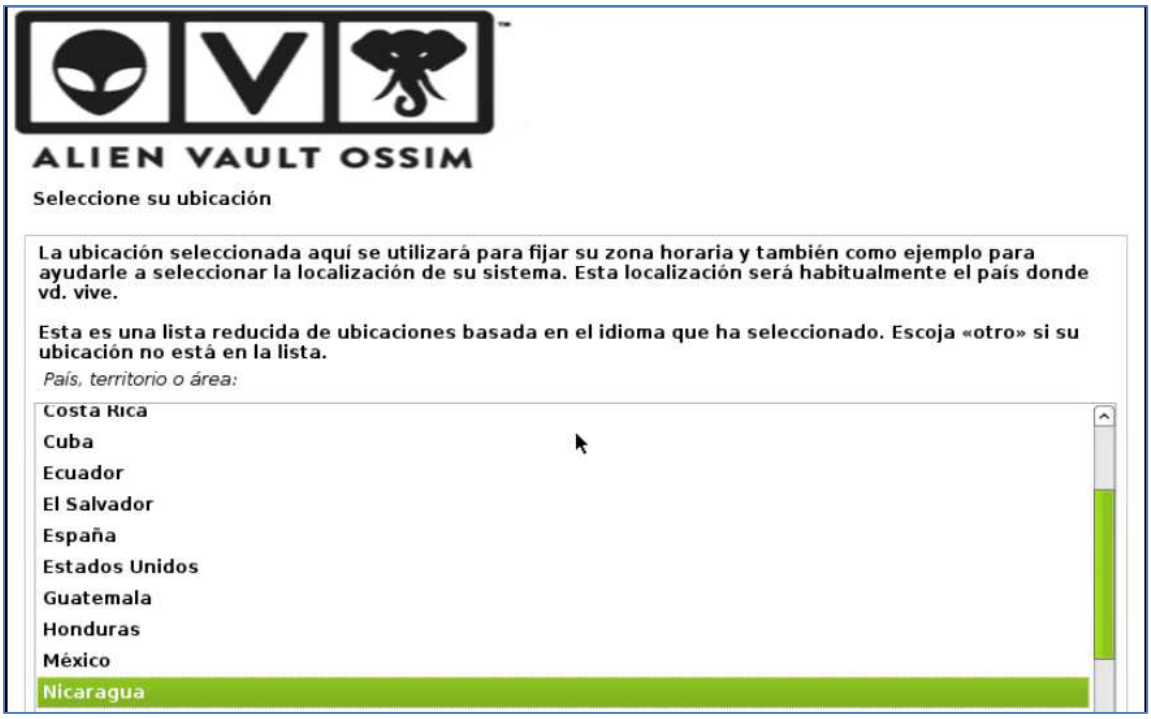


Figura No 33. Selección de ubicación geográfica (Captura de pantalla de equipo personal)

En la **Figura 34** se muestra la selección de idiomas para teclado y lo que debemos hacer es seleccionar el idioma español que gestionará el software.

Figura No 34. Selección idioma de teclado (Captura de pantalla de equipo personal)

Luego del idioma OSSIM inicia la carga de todos los componentes requeridos en la instalación mostrada en la **Figura No 35**.

Figura No 35. Progreso de descarga de componentes (Captura de pantalla de equipo personal)

Luego de la carga de componentes la **Figura No 36** muestra la información de los adaptadores de red encontrados en el equipo. En este caso se ha configurado tres adaptadores en el hardware virtual. Se selecciona la interfaz que llevará a cabo la tarea de administración del OSSIM. Las otras dos interfaces tendrán otros propósitos que serán explicados durante una de las fases de instalación que continúa más adelante.

Figura No 36. Selección de adaptador de red (Captura de pantalla de equipo personal)

A partir de este momento se inicia la reconfiguración de la interfaz de red eth0 que seleccionamos como interfaz de administración. La **Figura No 37** muestra la configuración del número IP a utilizar. En este caso el IP 192.168.8.222

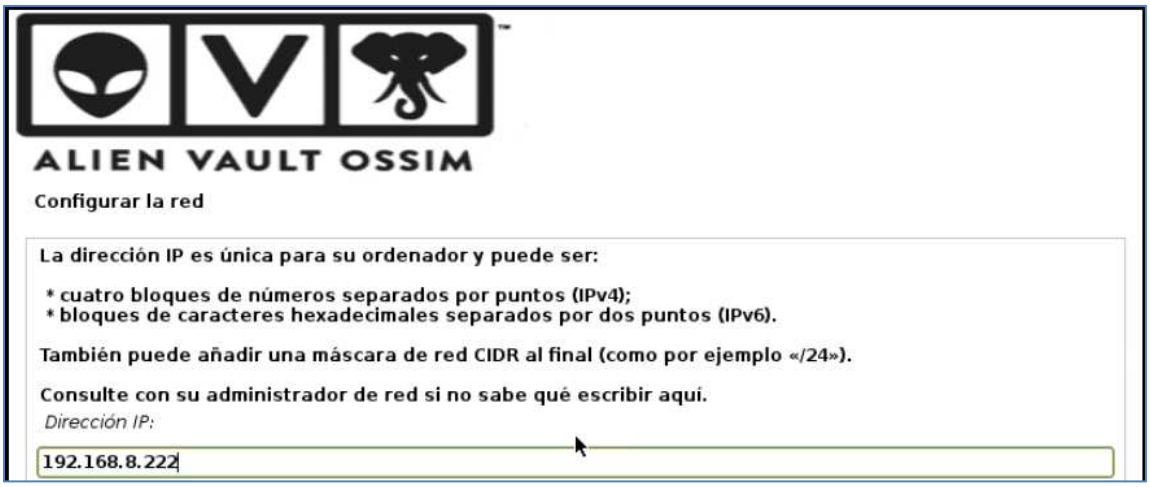


Figura No 37. Configuración IP OSSIM (Captura de pantalla de equipo personal)

En la **Figura No 38** se muestra configuración de la máscara de red. En este caso 255.255.255.128 ya que es parte de un segmento de direcciones IP que van del 192.168.8.129 al 192.168.8.254.

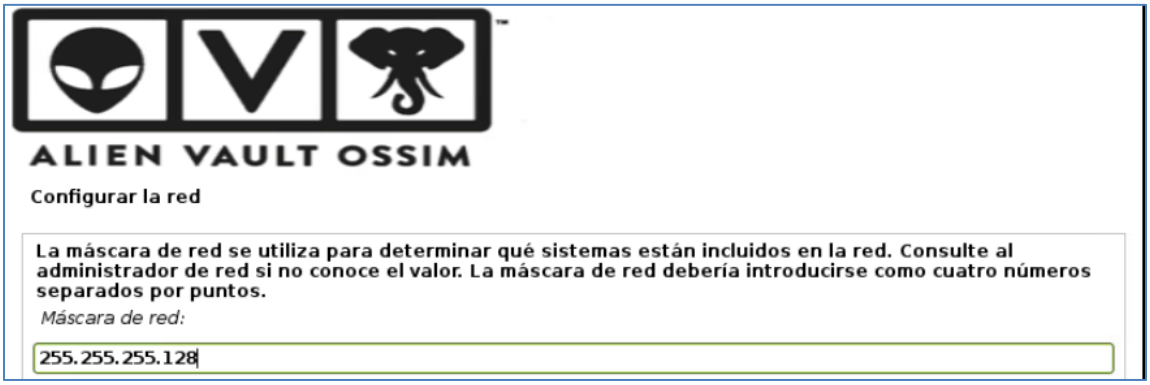


Figura No 38. Configuración Mascara de Red OSSIM (Captura de pantalla de equipo personal)

La **Figura No 39** muestra el IP que se coloca en la de la puerta de enlace. En caso de no colocarse una puerta de enlace el equipo a nivel administrativo solo será visto por el segmento al que pertenece. En esta caso se define el IP de la puerta de enlace como 192.168.8.129, dejando por tanto visible la administración a nivel de todas las redes. Aunque a nivel interno por motivos de seguridad las redes que forman parte de la VLAN solo pueden verse entre ellas en ciertos IP que han sido previamente configurados en el Router por motivo de configuraciones de seguridad.

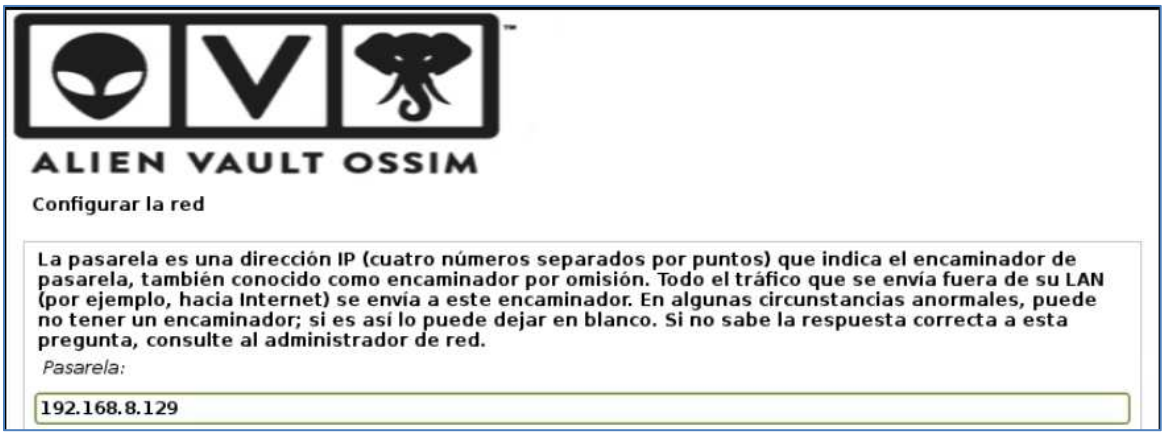


Figura No 39. Configuración Puerta de Enlace para OSSIM (Captura de pantalla de equipo personal)

La **Figura No 40** muestra la dirección del servidor de nombres de dominio configurado para el OSSIM. En nuestro caso por motivos de seguridad se utilizara el servidor DNS de "google" ya que a nivel interno las configuraciones de estos equipos no pueden ser reveladas.

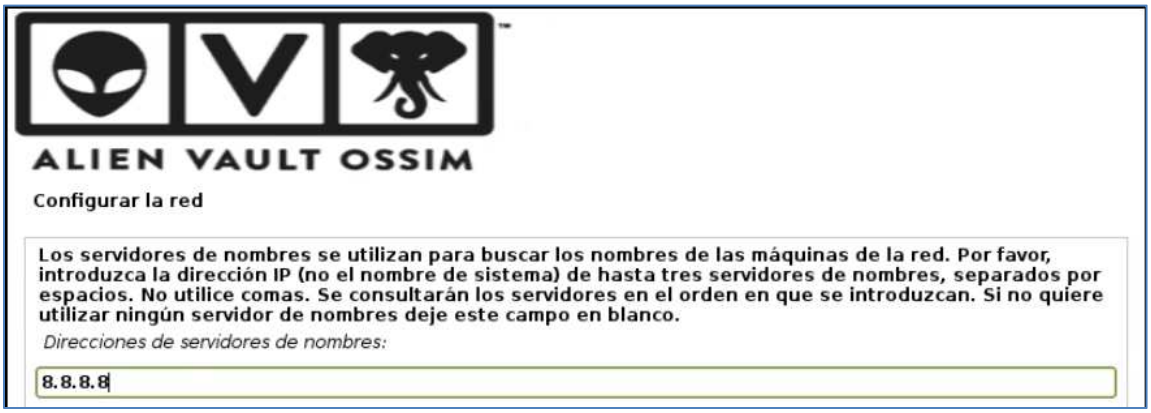


Figura No 40. Configuración de DNS para OSSIM (Captura de pantalla de equipo personal)

Ahora en la **Figura No 41** lo que se configura es la contraseña del usuario "root". El OSSIM es una versión de Linux (Debian 4.9.168-1+deb9u3~deb8u1 (2019-06-17) x86_64) adecuada con el propósito de utilizarse para el SIEM.

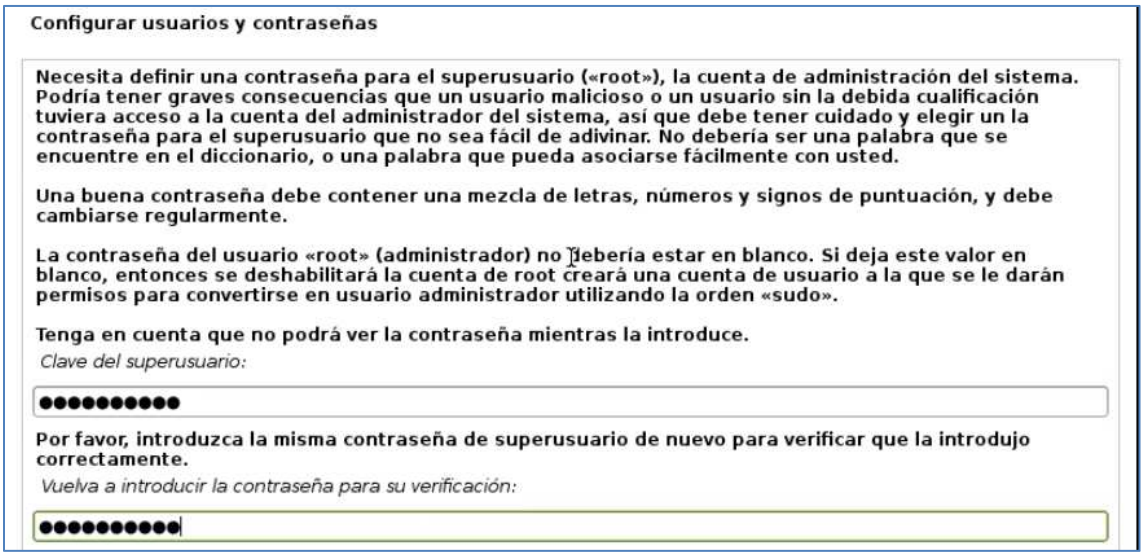


Figura No 41. Establecimiento de Credenciales para OSSIM (Captura de pantalla de equipo personal)

Con la clave del usuario "root" ya configurado inicia el proceso de instalación de todos los componentes mostrado en la **Figura No 42**.

Figura No 42. Configuración de sistema base en progreso (Captura de pantalla de equipo personal)

Figura No 43. Finalizando instalación OSSIM (Captura de pantalla de equipo personal)

El proceso de instalación total es de aproximadamente de 30 minutos. Este tiempo puede variar en dependencia del hardware utilizado. Parte del proceso es mostrado en la **Figura No 43**. Con la instalación completada inicia la carga de OSSIM mostrada en la **Figura No 44**. Cuando la carga está completa muestra una terminal de Linux, ver **Figura No 45**.

Figura No 44. Pantalla de OSSIM en su inicio. (Captura de pantalla de equipo personal)

La carga de AlienVault OSSIM ha sido completada mostrada en la consola de la **Figura No 45**. Lo que toca hacer ahora es abrir el navegador de su preferencia y escribir la dirección IP del OSSIM utilizando https://192.168.8.222

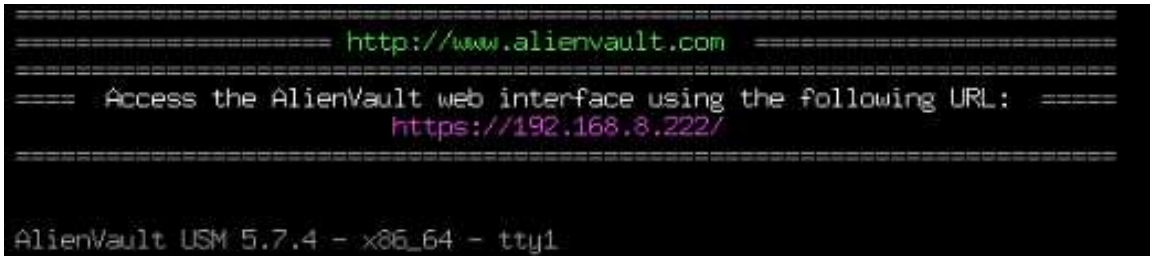


Figura No 45. Consola de OSSIM (Captura de pantalla de equipo personal)

Cuando la instalación está completa y accedemos al URL de la **Figura No 45** se brinda la primera interfaz del OSSIM para la creación del usuario "admin". Este usuario será el que vía web tendrá privilegio de administración sobre la plataforma del SIEM. Para este efecto escribimos en el campo "FULL NAME", en español nombre completo, Diego Manuel Vega Amoretti. Luego en el campo "PASSWORD", en español contraseña, establecemos la clave del usuario "admin". En el campo "EMAIL", en español correo electrónico, establecemos la dirección dmvega@eaai.com.ni, que será utilizado para envío de alertas; en el campo "COMPANY NAME", en español nombre de la compañía o negocio, se escribe las siglas de la empresa EAAI. Finalmente se escribe en el campo "LOCATION", en español ubicación Nicaragua y automáticamente establece el software la ubicación geográfica en Managua, Nicaragua. Ver **Figura No 46**, ahora con todos esos campos solo se hace clic en el botón "START USING ALIEN VAULT".

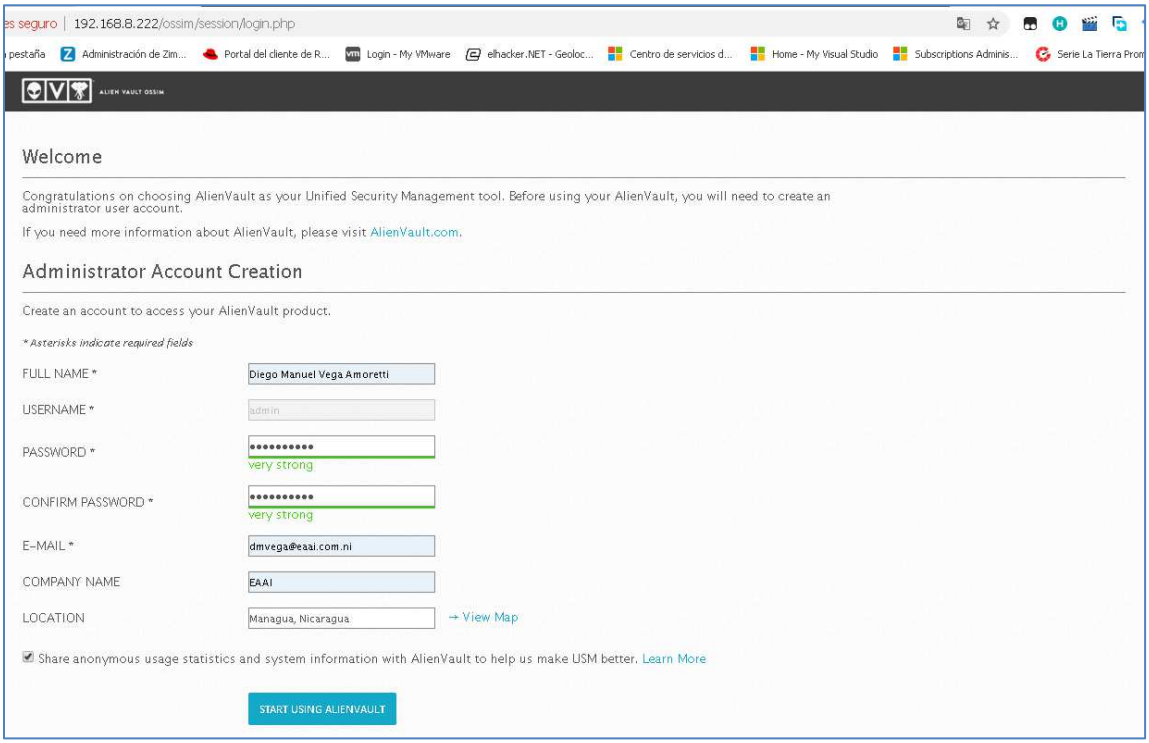


Figura No 46. Pantalla Web de configuración de usuario OSSIM (Captura de pantalla de equipo personal)

Después de establecer al usuario "admin" aparece una pantalla de bienvenida con un asistente mostrado en la **Figura No 47** para configurar los primeros elementos de OSSIM. En nuestro caso hacemos clic en "START" para iniciar el asistente.

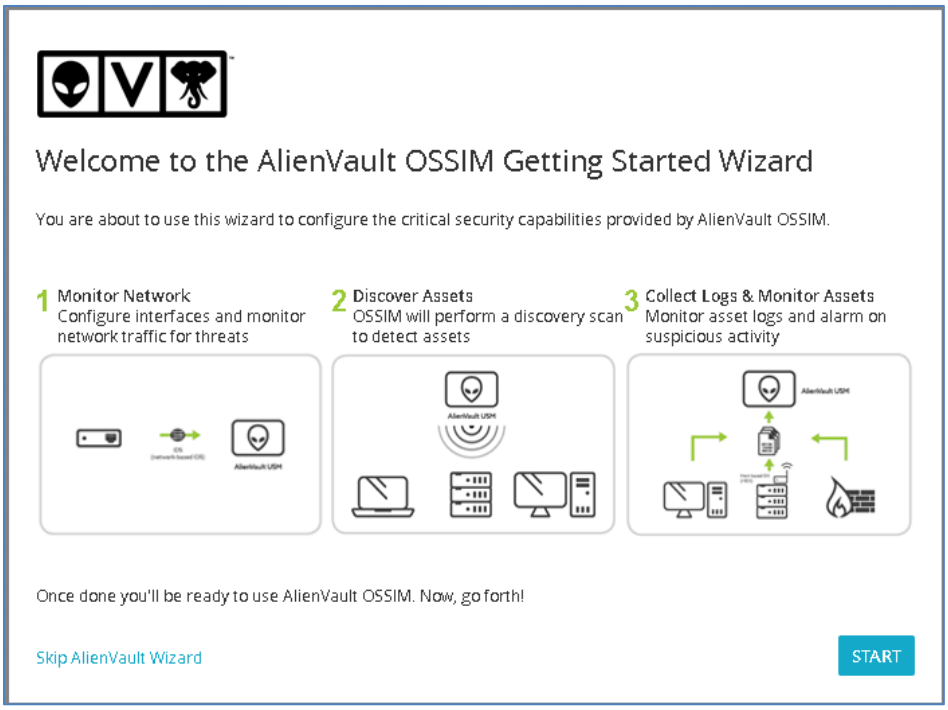


Figura No 47. Pantalla de inicio de OSSIM (Captura de pantalla de equipo personal)

El asistente consta de cinco etapas. La primera etapa es la configuración de las otras dos interfaces del equipo virtual. En este punto establecemos la eth1 como monitoreo de red. La interfaz eth2 es utilizada para recibir Log y búsqueda de activos. En la **Figura No 48** se establece el IP 192.168.0.59 para la eth2, luego hacemos clic en "NEXT" para ir a la siguiente etapa.

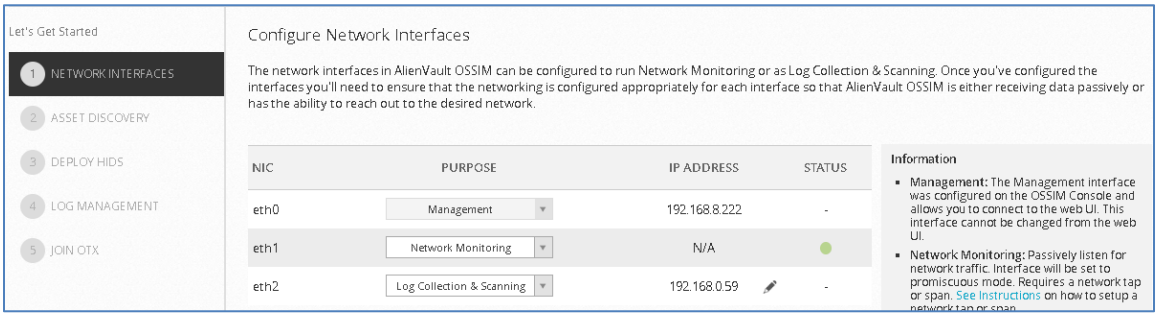


Figura No 48. Configuración de interfaces de OSSIM (Captura de pantalla de equipo personal)

Después de haber configurado las interfaces de red restantes se procede a la segunda etapa, mostrada en la **Figura No 49**, que es el descubrimiento de activos. En esta etapa por defecto el software realizó una búsqueda de los activos de la red que son parte de los segmentos de red de las interface eth0 y eth2. En esta etapa podemos además agregar más redes o modificar los

elementos actualmente encontrados. En nuestro caso procedemos a agregar más redes. Para esto hacemos clic en "SCAN NETWORK", en español búsqueda de redes.

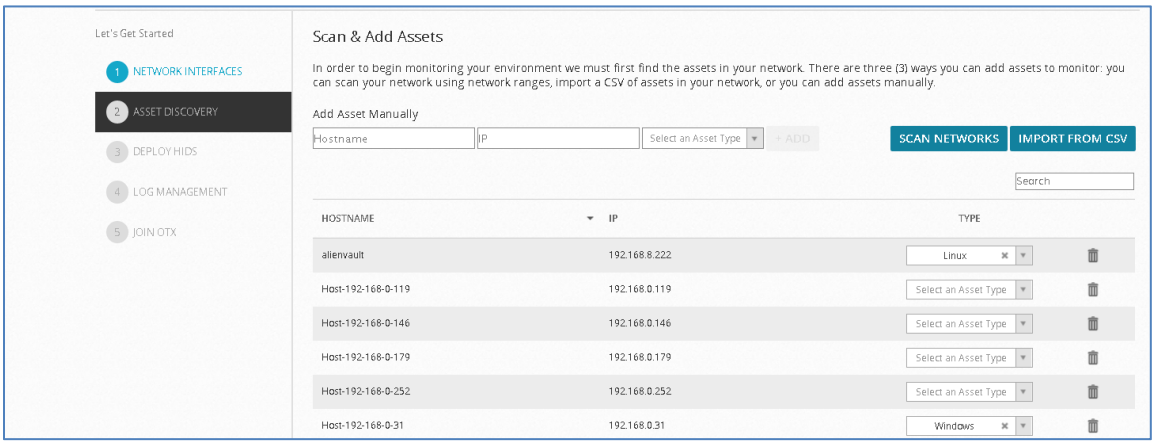


Figura No 49. Configuración de escaneo de redes y activos. (Captura de pantalla de equipo personal)

En la **Figura No 50** observamos la opción de **SCAN NETWORKS.** Una vez abierto el asistente de la **Figura No 51** procedemos a hacer clic en "IMPORT FORM CSV", en español importar de "csv" (formato de archivo separado por coma o punto y coma).

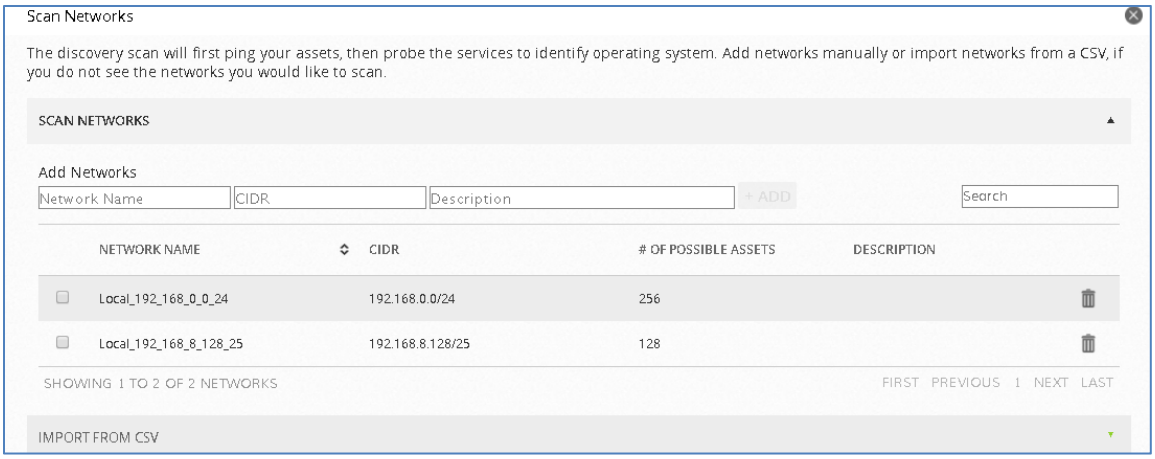


Figura No 50. Selección para Importar redes (Captura de pantalla de equipo personal)

El archivo que vamos a importar se llama "REDES PARA OSSIM.txt", el formato en el cual se agregan las redes es tal como se describe en el asistente entre comillas se escriben los campos y se separan por "punto y coma".

En la **Figura No 52** nos muestra el nombre de archivo importado cuando se hizo clic en "Seleccionar archivo".

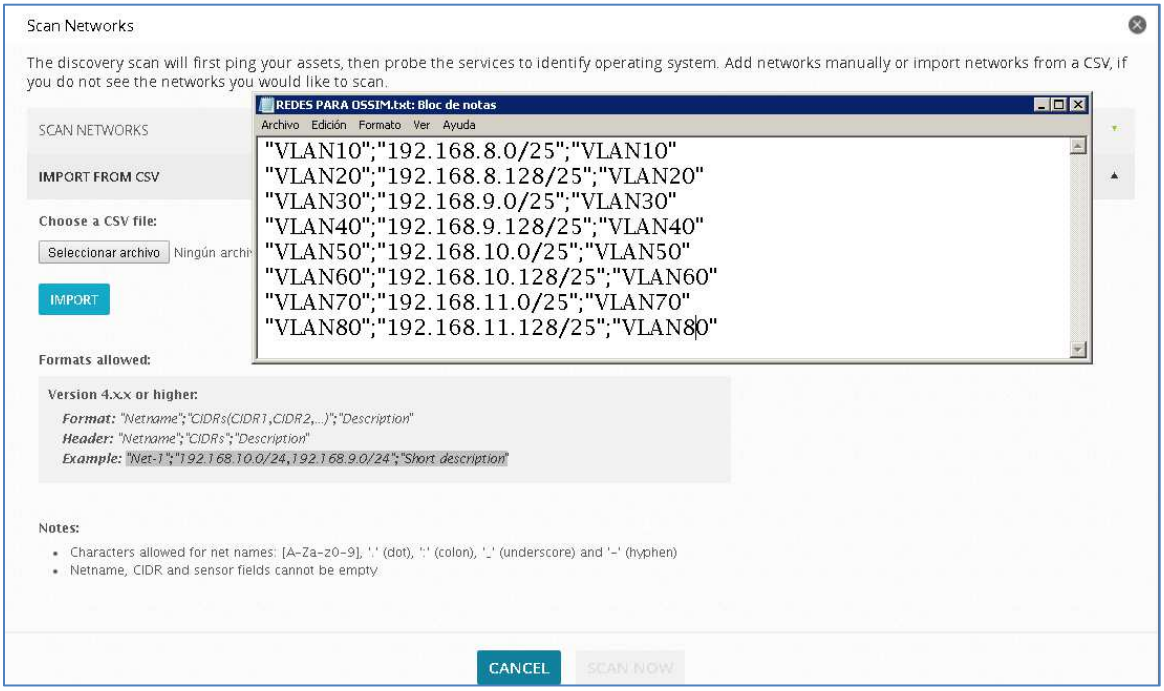


Figura No 51. Agregando Archivo con redes de la EAAI (Captura de pantalla de equipo personal)

Con el archivo ya seleccionado hacemos clic en "IMPORT", en español importar.

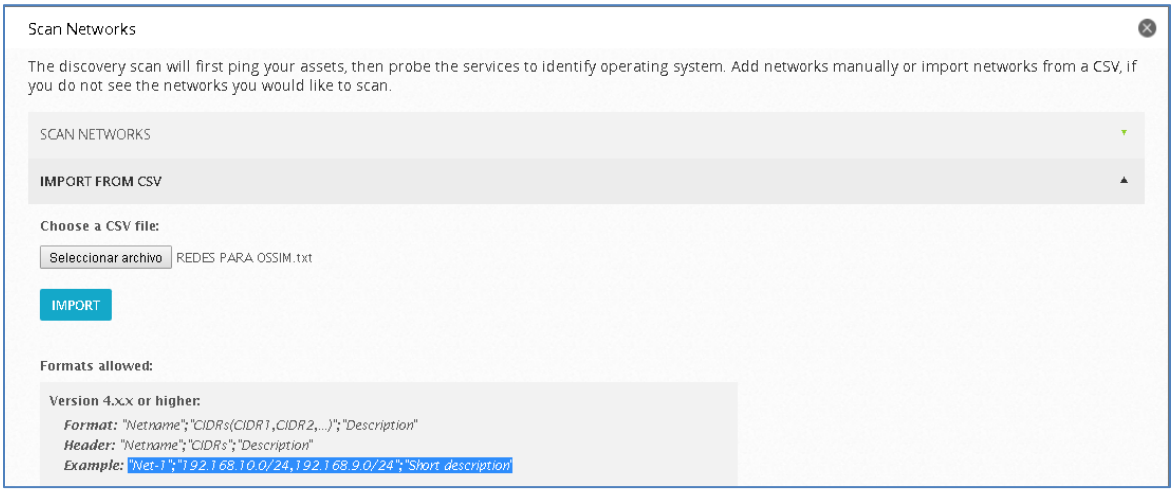


Figura No 52. Archivo de Redes adjuntado en OSSIM (Captura de pantalla de equipo personal)**.**

La información del archivo ha sido importada con éxito y se han definido un total de 8 redes mostradas en la **Figura No 53** y **Figura No 54** (Captura de pantalla de equipo personal).

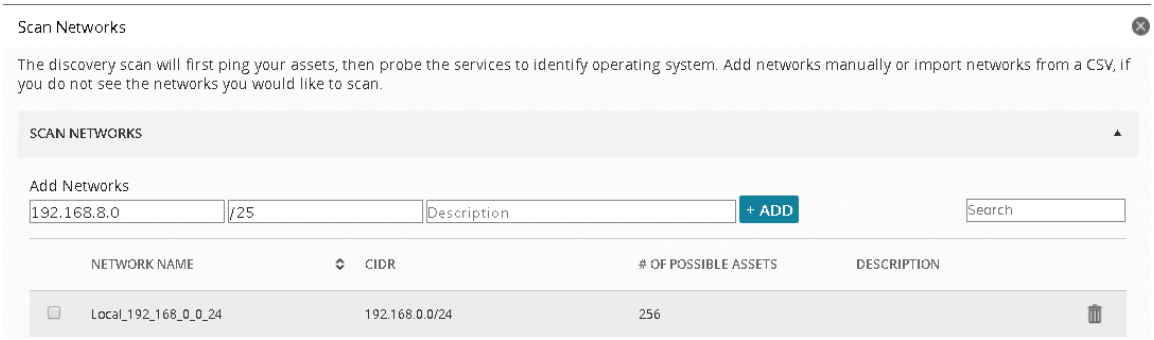


Figura No 53. Redes detectadas (Captura de pantalla de equipo personal)

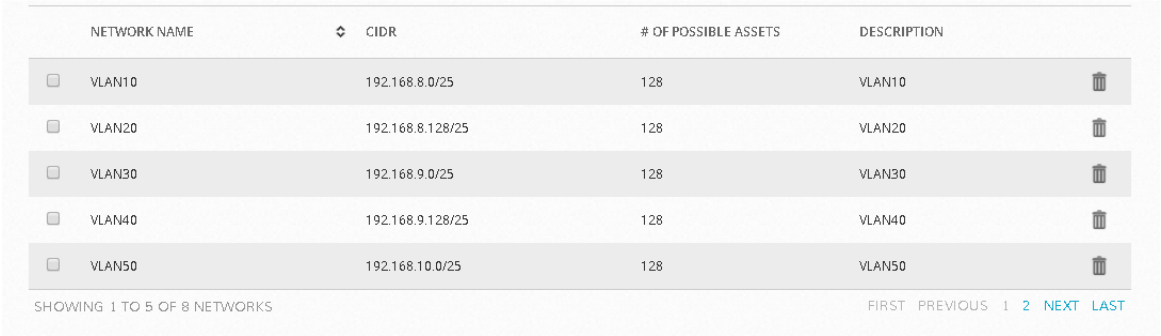


Figura No 54. Redes detectadas (Captura de pantalla de equipo personal)

En la **Figura No 53** y **Figura No 54** observamos todas las redes; pero como hay aún redes eliminaremos la local_192_168_0_0_24 y crearemos una regla que incluya toda la LAN nativa, 192.168.0.0/24 hasta la red 192.168.3.0/24. Se puede observar en la **Figura 55** que la LAN 192.168.0.0/24 ha sido eliminada.

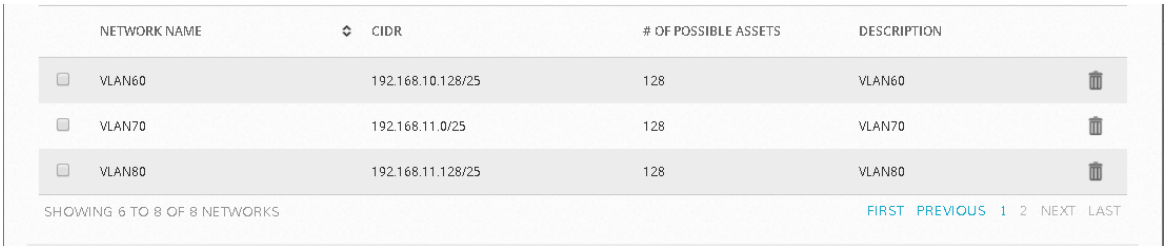


Figura No 55. Red Eliminada en OSSIM (Captura de pantalla de equipo personal)

En la **Figura No 56** se observa que la VLAN a crearse se denomina "VLAN NATIVA". Esta contiene las redes 192.168.0.0/24-192.168.3.0/24.

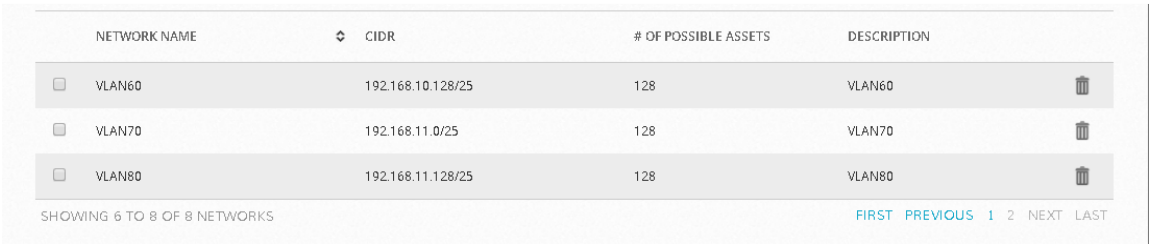


Figura No 56. VLANs Creadas en OSSIM (Captura de pantalla de equipo personal)

La red VLAN_NATIVA ha sido creada con éxito. Ahora si podemos seleccionar todas las redes creadas y hacer clic en "SCAN NOW", en español buscar ahora. Tal como se observa en la **Figura No 57**.

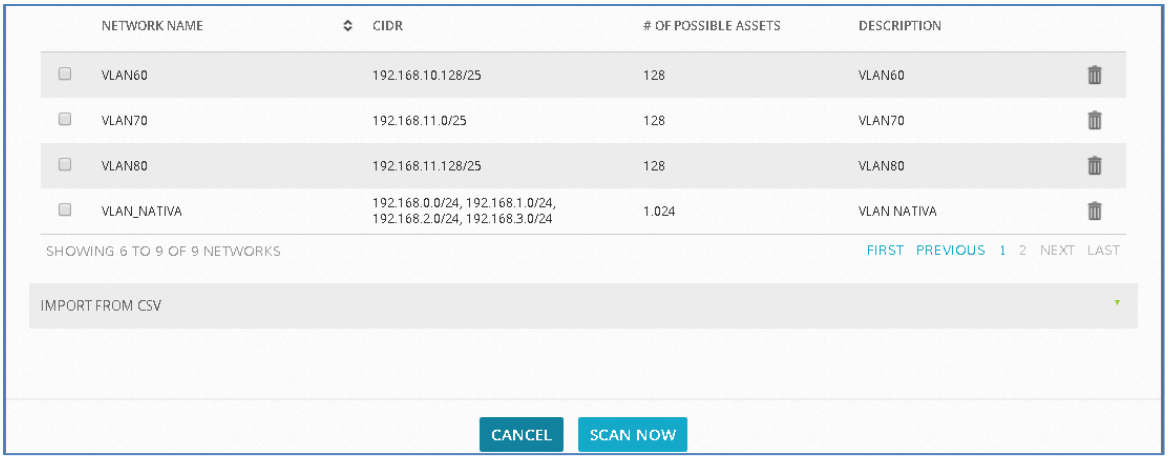


Figura No 57. Escaneo de Redes en OSSIM (Captura de pantalla de equipo personal)

En estos momentos aparece un cuadro de dialogo en la **Figura No 58** preguntando si estamos seguros de realizar una búsqueda de 2048 direcciones IP, nos informa que esto llevará más que unos pocos minutos.

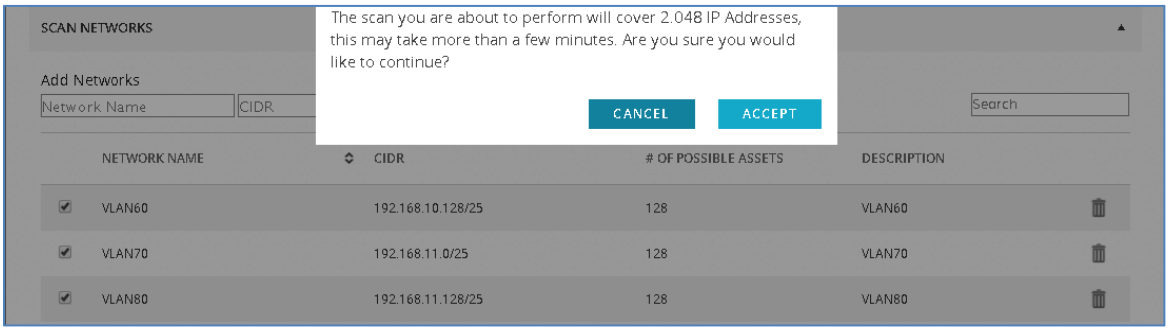


Figura No 58.Confirmación para escaneo de red (Captura de pantalla de equipo personal)

El proceso de descubrimiento de activos ha iniciado. Ver **Figura No 59.**

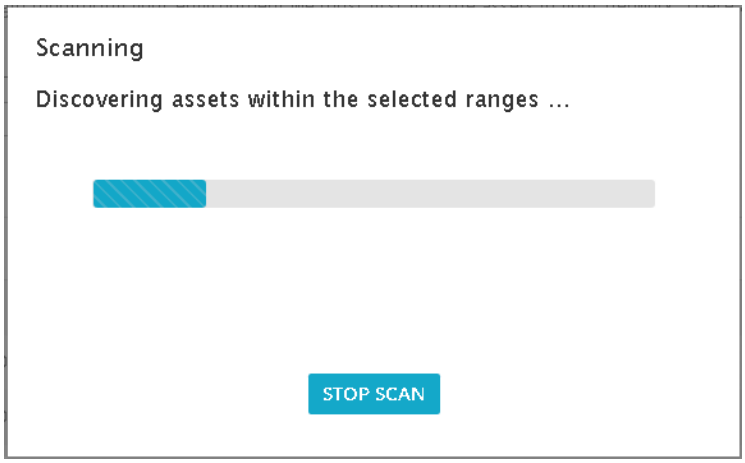


Figura No 59. Inicio de proceso de descubrimiento de activos (Captura de pantalla de equipo personal)

Una vez que el proceso de búsqueda y descubrimiento de activos ha iniciado el asistente intentará identificar la versión del sistema operativo de ser posible. Si al final no detecta la versión da la opción a que nosotros se la digamos. En la **Figura No 60** nos dice que la cantidad de 2048 redes puede durar hasta 6 horas y 36 minutos.

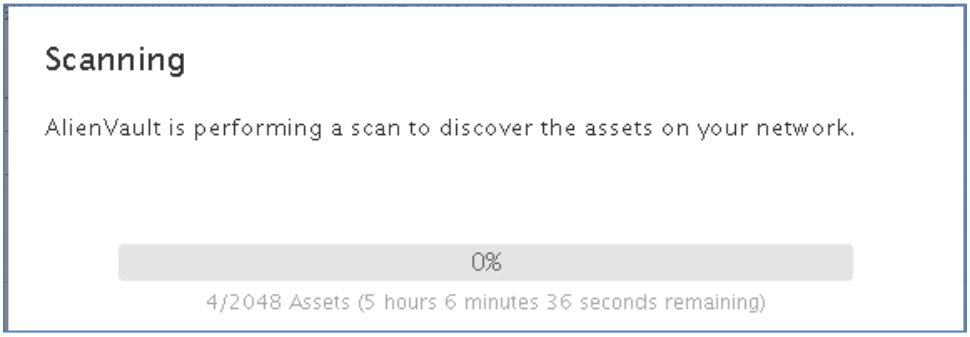


Figura No 60. Tiempo de escaneo de redes

El progreso de la búsqueda es bastante lento. En la **Figura No 61** se muestra que lleva sólo 240 host y faltan 3 horas y 30 minutos.

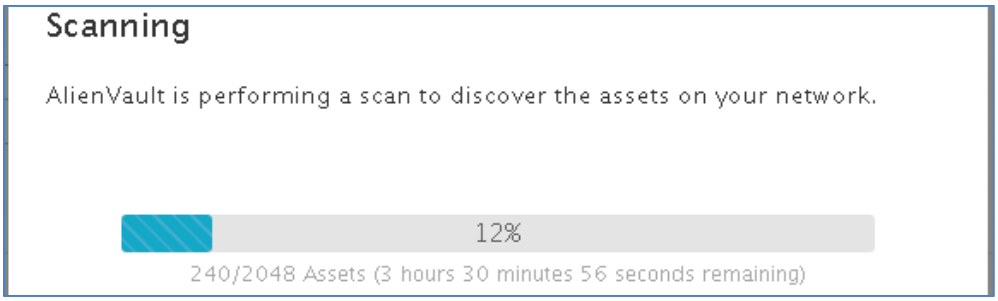


Figura No 61. Escaneo al 12 por ciento (Captura de pantalla de equipo personal)

Finalizado el descubrimiento se muestra la información recabada. **Ver Figura No 62**.

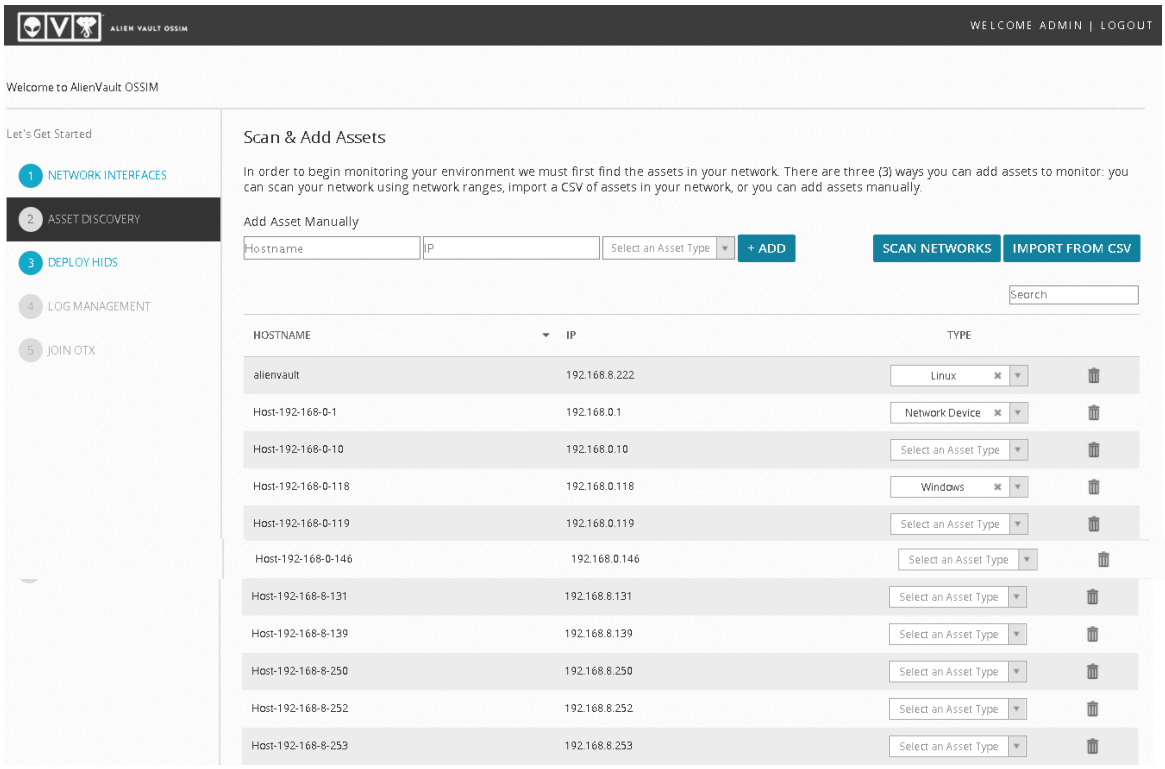


Figura No 62. Extracto de información escaneada (Captura de pantalla de equipo personal)

Como se ha podido observar en la **Figura No 62** durante esta etapa se han detectado varios host de las distintas redes. Lo que ahora sigue es el proceso de instalación de los agentes en los equipos que se seleccionen para la prueba. En esta tercera etapa del asistente post instalación se procede a realizar la instalación remota del agente en los equipos Windows. Para esto hemos seleccionado dos equipos. Una estación de trabajo de monitoreo y un servidor virtual temporal con copia de solo lectura de las cuentas de dominio. Para esto se debe proporcionar datos de usuario con privilegios en el dominio. Se ha

creado un usuario temporal con privilegios de administrador en los equipos dados. En el campo "Username" (Nombre de Usuario en español) se escribe "**Melquisedec**", en el campo "Password" (Clave o contraseña en español) la clave de la cuenta ********** y en el campo "Domain" (Dominio en español) se escribe el nombre del dominio; en este caso AIMACS. Luego en "Deploy to the following host" (En español: Implementar a los siguientes equipos) se seleccionan los IP de los equipos a los cuales se instala el agente **HIDS** (Host Intrusion Detection System, en español Sistema de detección de intrusos en un equipo). Una vez llenado y seleccionado los datos requeridos se procede a hacer clic en "DEPLOY" (en español implementar) para iniciar el proceso de despliegue del agente HIDS. Tal como se muestra en la **Figura No 63**.

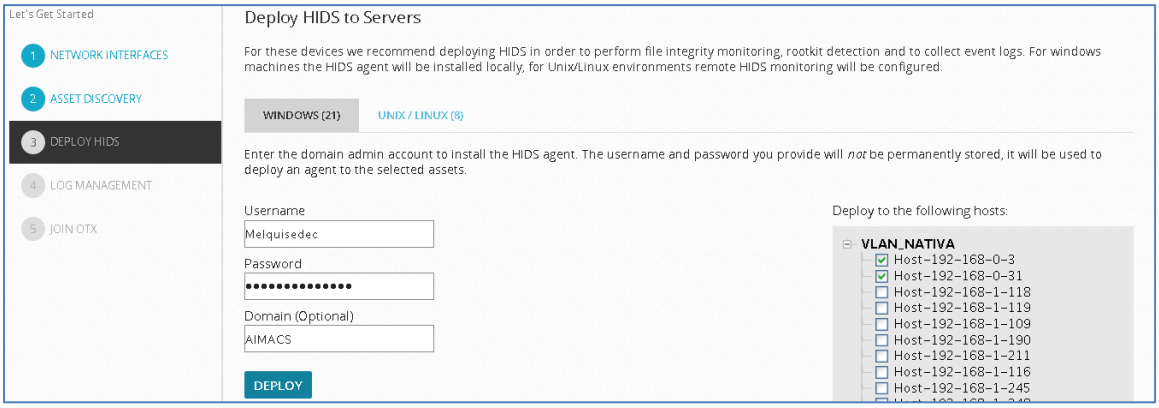


Figura No 63. Despliegue de agente HIDS en Windows (Captura de pantalla de equipo personal)

Luego de hacer clic en "DEPLOY" nos pregunta si estemos seguros de iniciar el despliegue del agente "HIDS" en dos equipos, tal como se muestra en la **Figura No 64**. Para continuar el proceso seleccionamos "CONTINUE" (Continuar en español).

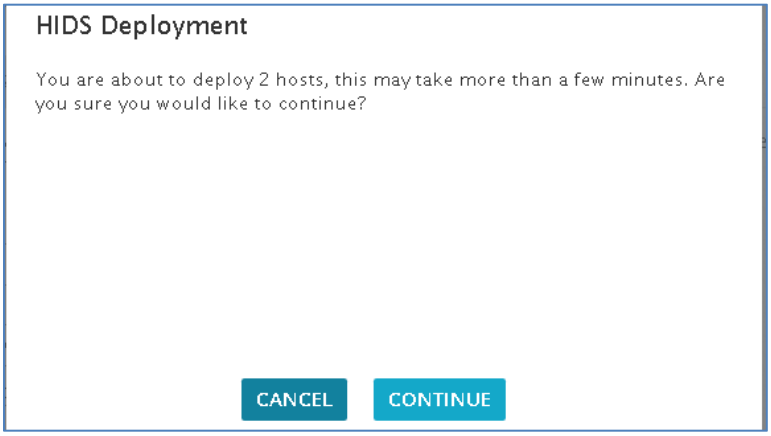


Figura No 64. Confirmación de despliegue de agente en Windows (Captura de pantalla de equipo personal)

El proceso ha iniciado y estamos a esperas de los resultados.

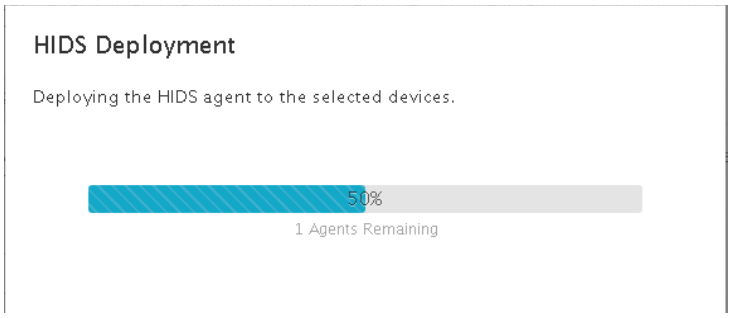


Figura No 65. Progreso de instalación de HIDS Windows (Captura de pantalla de equipo personal)

Después de un tiempo de espera en la **Figura No 65** el proceso en esta etapa ha fallado, pues lo que ha hecho es solo copiar el agente en el equipo destino pero no hizo el despliegue completo. En el apartado **5.5 Integración de Sensores** se realizará la instalación manual y explicaremos el motivo de la falla. Nuestro siguiente paso es realizar la instalación a nivel de Linux, utilizaremos el servidor de LOG. Proporcionamos un usuario con privilegios de conexión para utilizar ssh. Para este efecto en el campo "SSH Username" (en español usuario SSH) escribimos root y en el campo "SSH Password" (en español contraseña SSH) escribimos la contraseña **********. Tal como se muestra en la **Figura No 66**. Cabe mencionar que una práctica de seguridad correcta es ***impedir a los usuarios el uso del root para conexiones ssh***. Por efectos de prueba hemos permitido la utilización de root para ssh para demostrar que el tipo de usuario requerido para el despliegue del agente debe tener privilegios de root. Luego de llenar esos datos y hacer seleccionar en "Deploy to the following hosts" (en español implementar a los siguientes equipos) el equipo al que deseamos instalar el agente procedemos presionar el botón "DEPLOY" (en español implementar).

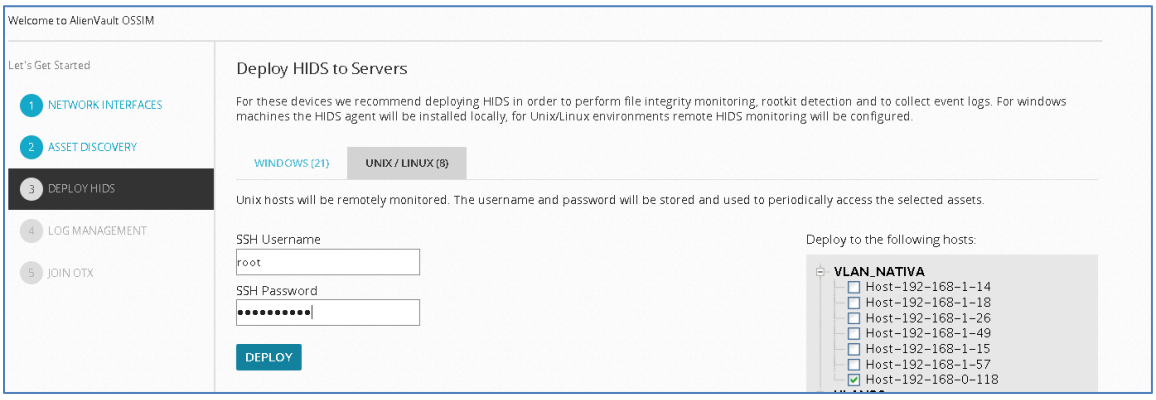


Figura No 66. Configuración de credenciales para agente HIDS en Linux (Captura de pantalla de equipo personal)

Luego del clic en "DEPLOY" nos confirman si estamos seguros de procedes con la instalación del agente. Respondemos continuar haciendo clic en "CONTINUE", igual que en la **Figura 64**. El proceso es similar pero en este caso el resultado es satisfactorio, ver **Figura No 67**.

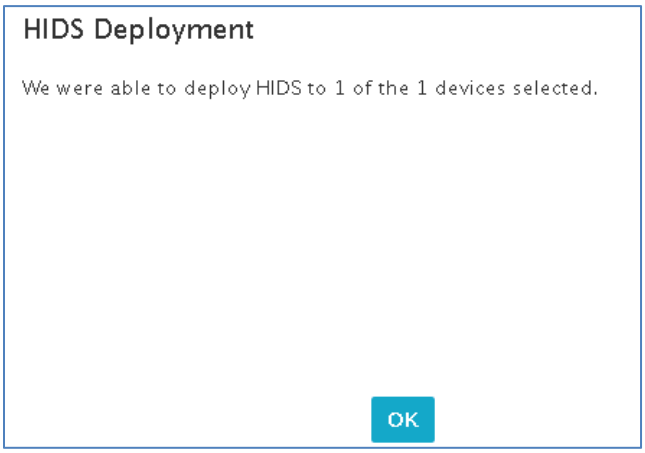


Figura No 67. Despliegue de agente en Linux completo (Captura de pantalla de equipo personal)

La **Figura No 68** muestra la cuarta etapa del asistente inicial del OSSIM consiste en configurar el manejo de LOG de dispositivos de red. En este caso el asistente ha detectado 4 equipos de red que son posibles fuentes de LOG. Para activar está opción de recibir los LOG de los agentes se debe hacer todo lo descrito en el apartado "8.3 CONFIGURACIONES PREVIAS A SENSORES". Lo que ahora sigue es seleccionar equipo como el IP 192.168.0.253 y 192.168.0.1; a esos equipos se les configura en "VENDOR" (En español vendedor o fabricante) la marca del equipo, en "MODEL" (En español modelo) el tipo de equipo según la marca. Con los datos requeridos configurados hacemos clic en "ENABLE" (En español habilitar).

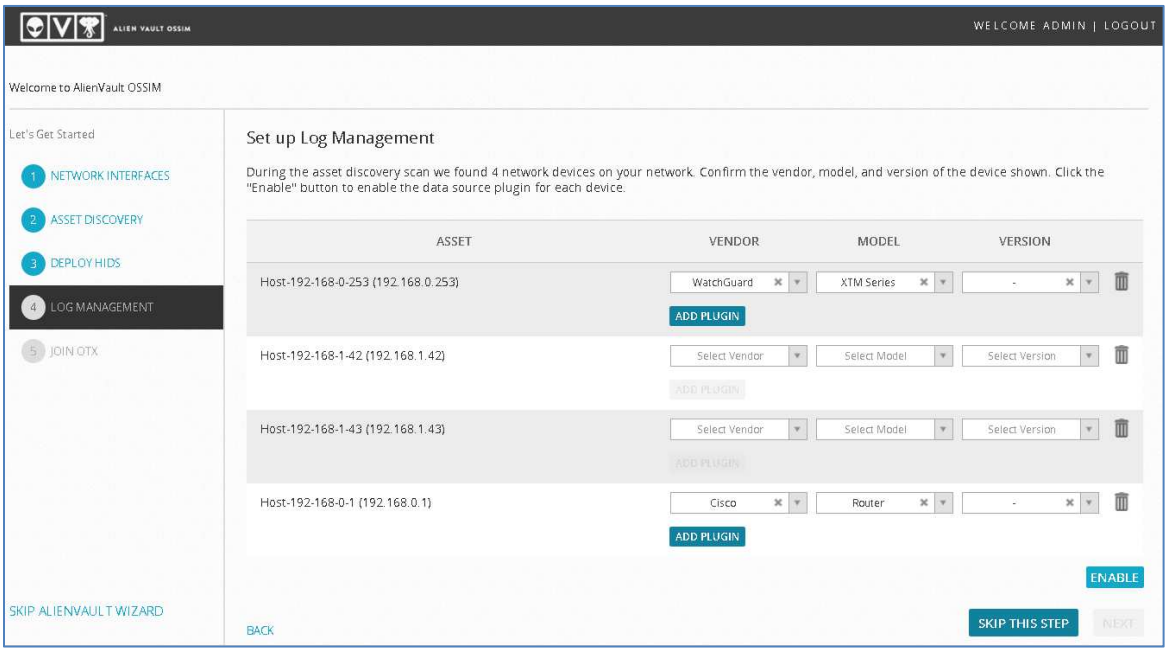


Figura No 68. Habilitar complemento syslog para equipos de red (Captura de pantalla de equipo personal)

Ahora se está comprobando en cada equipo si están configurados para enviar LOG a equipos remotos. Debemos por tanto esperar hasta que donde dice "PLUGIN ENABLED" (En español complemento habilitado) esté con indicadores establecidos en verde. Tal como se muestra en la **Figura No 69**.

Figura No 69. Comprobando que Syslog este habilitado en los equipos (Captura de pantalla de equipo personal)**.**

En la **Figura No 70** OSSIM muestra Complemento Habilitado ("PLUGIN ENABLED"), el Router está enviando LOG de forma correcta. Aún se está a espera del equipo WatchGuard.

Figura No 70. Complemento habilitado en Router (Captura de pantalla de equipo personal)

Después de un tiempo de espera en la **Figura No 71** se muestran los dos equipos enviando LOG al OSSIM, en este punto ya podemos hacer clic en NEXT (En español siguiente) para ir a la última etapa del asistente.

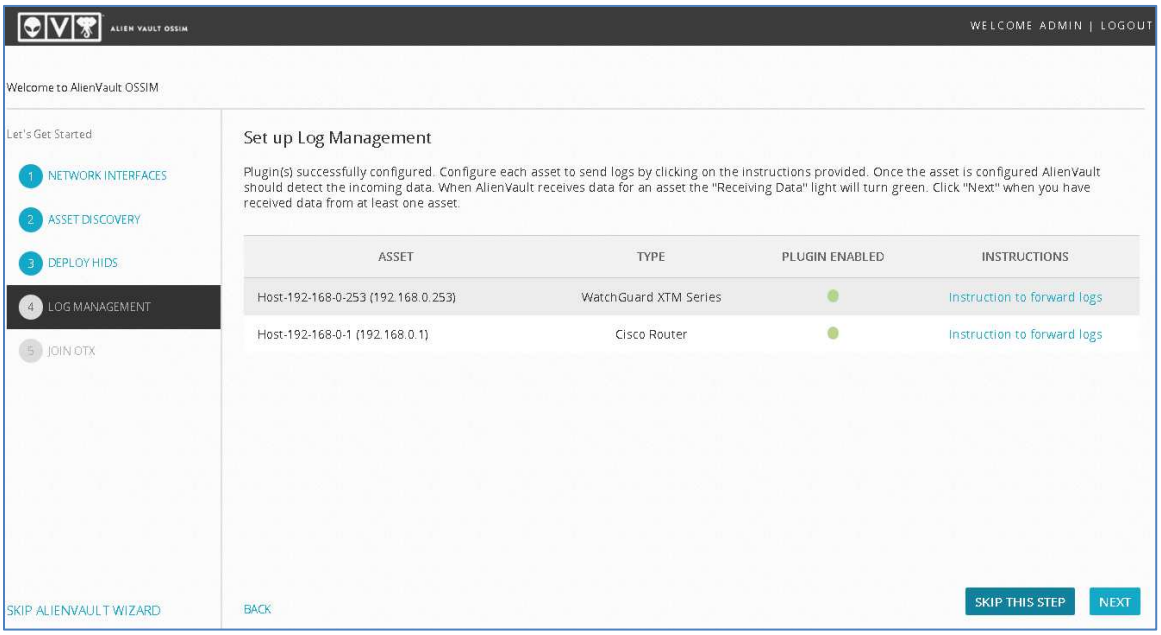


Figura No 71. Complemento habilitado en los dos equipos (Captura de pantalla de equipo personal)**.**

En esta quinta etapa y última etapa del asistente estamos en la opción de incluir en OSSIM la clave de **OTX** (Open Threat Exchange, en español intercambio abierto de amenazas). Para esto debemos tener creada una cuenta en el sitio de AlienVault. Para continuar y proporcionar la clave OTX para API (application programming interface, en español interfaz de programación de aplicaciones) hay que iniciar sesión haciendo clic en "SIGN UP NOW" (Regístrate ahora). Tal como muestra la **Figura No 72**.

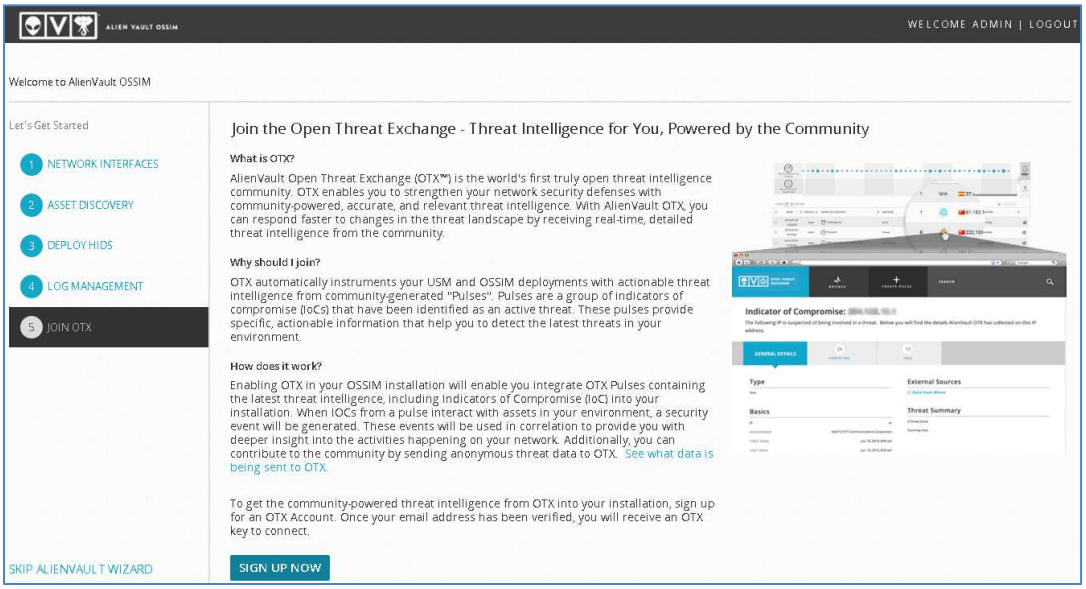


Figura No 72. Logueo en sitio web OTX (Captura de pantalla de equipo personal)

Ingresamos los datos en la ventana que aparece, ver **Figura No 73**; en el campo de "Username" (en español nombre de usuario) escribimos "diego.vega", en el campo "Password" (en español contraseña) la clave ********* del usuario registrado en OSSIM.

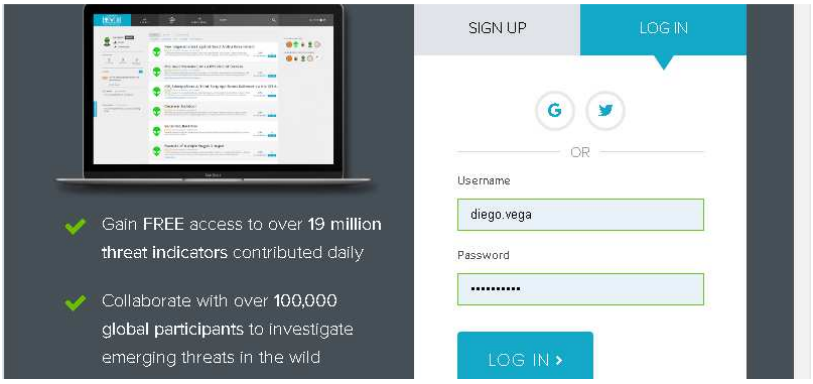


Figura No 73. Ingresando datos en sitio de OTX (Captura de pantalla de equipo personal)

La **Figura No 74** muestra que ya hemos ingresado, lo que debemos hacer es ir y buscar la opción donde aparece la clave de OTX. Hacemos clic en la opción "API Integration", (en español Integración de API) y copiamos la clave OTX de API. Tal como se observa en la **Figura No 75**.

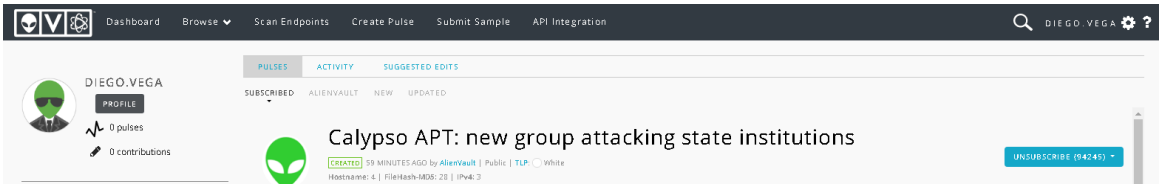


Figura No 74. Menú OTX

La clave de OTX que vamos a ingresar al OSSIM es: bea87fba2d4eb1b07dbaf2c04b07a64f91ac24ad61c36c97b0c9b71f8d3c5c0d

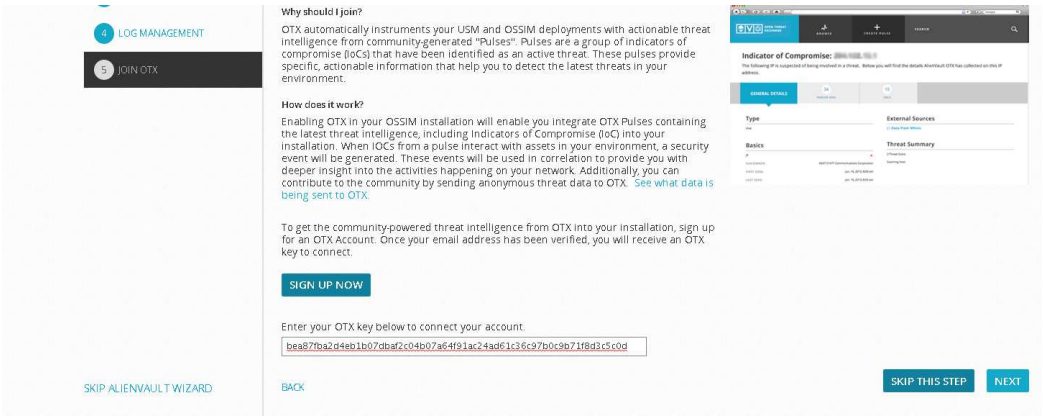


Figura No 75. Integración de API con clave OTX (Captura de pantalla de equipo personal)

Lo que ahora sigue es hacer clic en "NEXT" (en español siguiente) para finalizar el proceso de registro del OTX. Por otra parte en la **Figura No 76** se observa que nuestra cuenta ya está vinculada con el equipo OSSIM que configuramos.

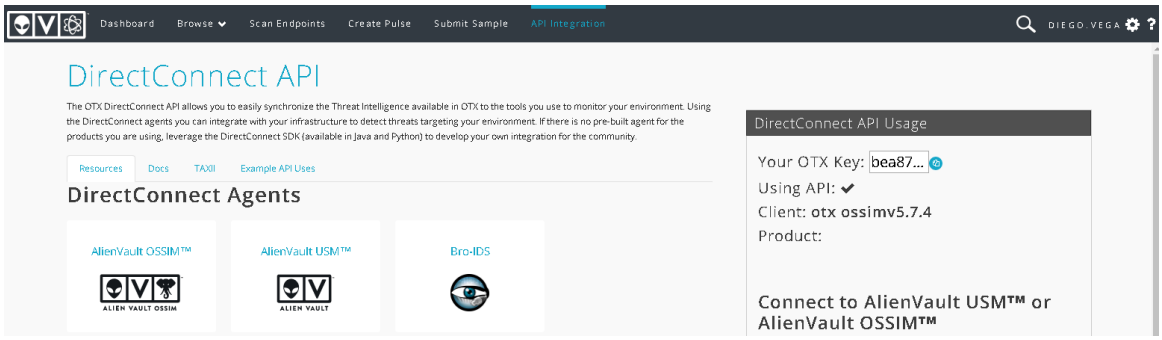


Figura No 76. API integrada con OSSIM 5.7.4

Lo que nos queda por hacer es dar clic en FINISH (en español finalizar), tal como se muestra en la **Figura No 77** (Captura de pantalla de equipo personal).

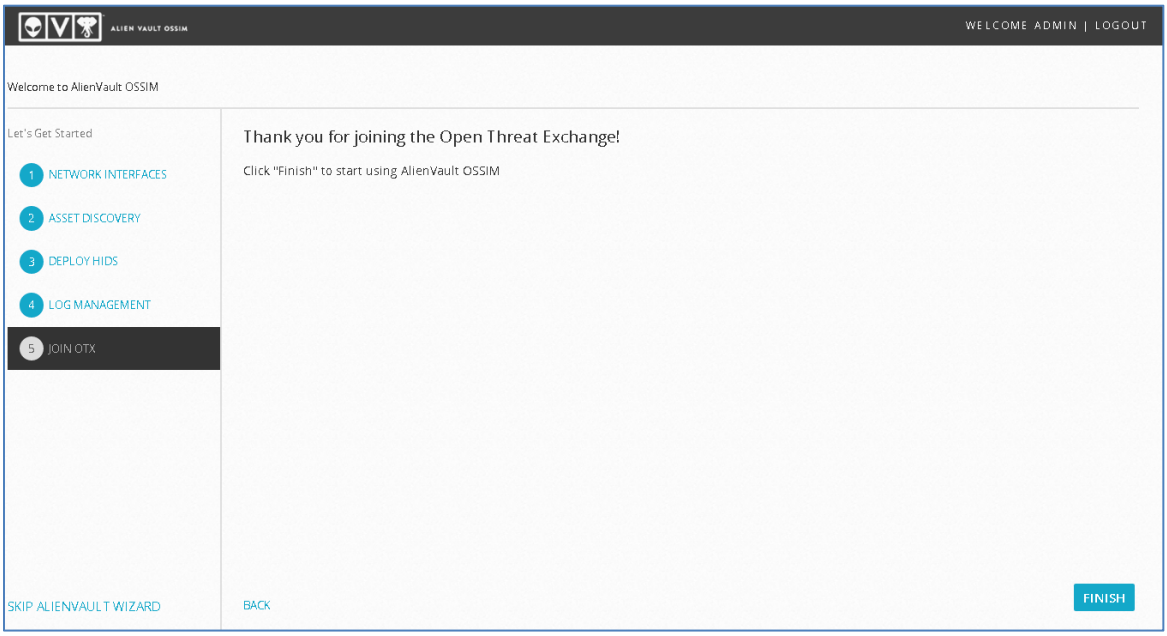


Figura No 77. Finalización asistente OSSIM (Captura de pantalla de equipo personal)

Como resultado aparece la ventana de felicitaciones en la **Figura No 78**. En este punto podemos configurar más fuentes de datos o hacer clic en explorar AlienVault OSSIM. En nuestro caso seleccionamos "EXPLORE ALIENVAULT OSSIM" (en español explorar AlienVault OSSIM).

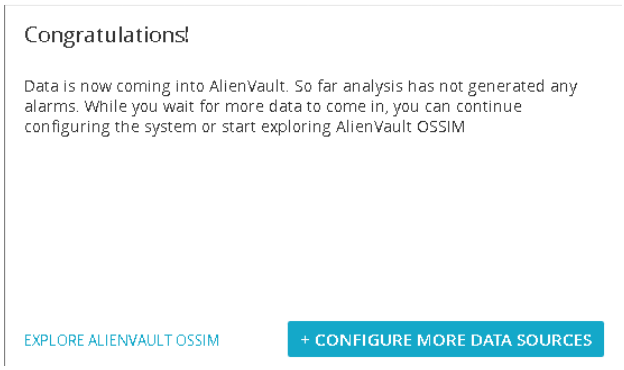


Figura No 78. Ventana de Felicitaciones OSSIM Completo (Captura de pantalla de equipo personal)

La primera pantalla de carga del OSSIM es el "DASHBOARDS" (en español cuadros de mando), en esta **Figura No 79** aparece un resumen de todo el comportamiento de la red detectado por OSSIM. Podemos observar en el sumario del cuadro de mando que existen cuatro opciones. La primera "EXECUTIVE" (en español ejecutivo) muestra los eventos generales detectados por el SIEM.

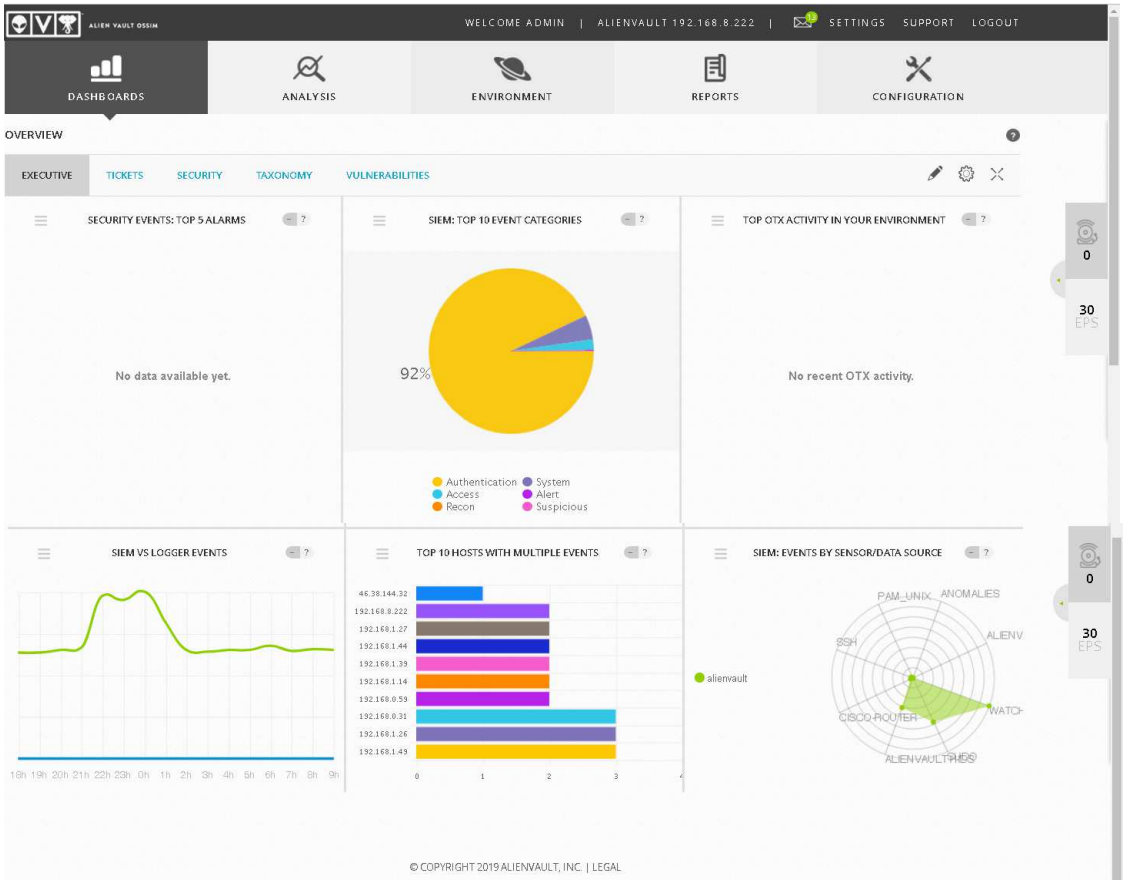


Figura No 79. Cuadro de Mando OSSIM (Captura de pantalla de equipo personal)

En los cuadros de mando (DASHBOARDS) también está la opción "DEPLOYMENT STATUS" (en español estado del despliegue), ver **Figura No 80**, donde se muestra el estado general de la implementación del SIEM.

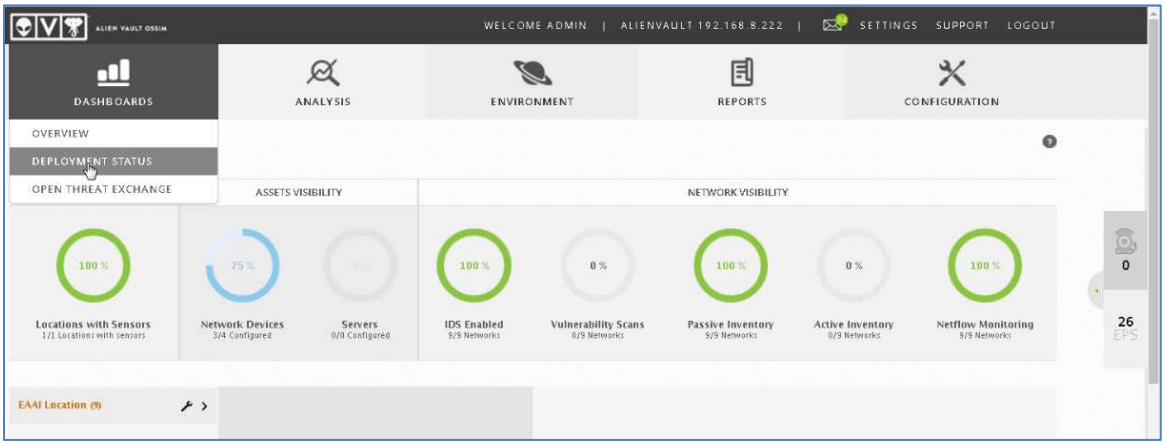


Figura No 80. Cuadro de Mando (Estado del Despliegue) (Captura de pantalla de equipo personal)

En los cuadros de mando (DASHBOARDS) existe la opción "OPEN THREAT EXCHANGE" (en español intercambio de amenaza abierta), ver **Figura No 81**. En esta opción se muestran los pulsos publicados por otros usuarios debido a las amenazas detectadas en otros sitios remotos.

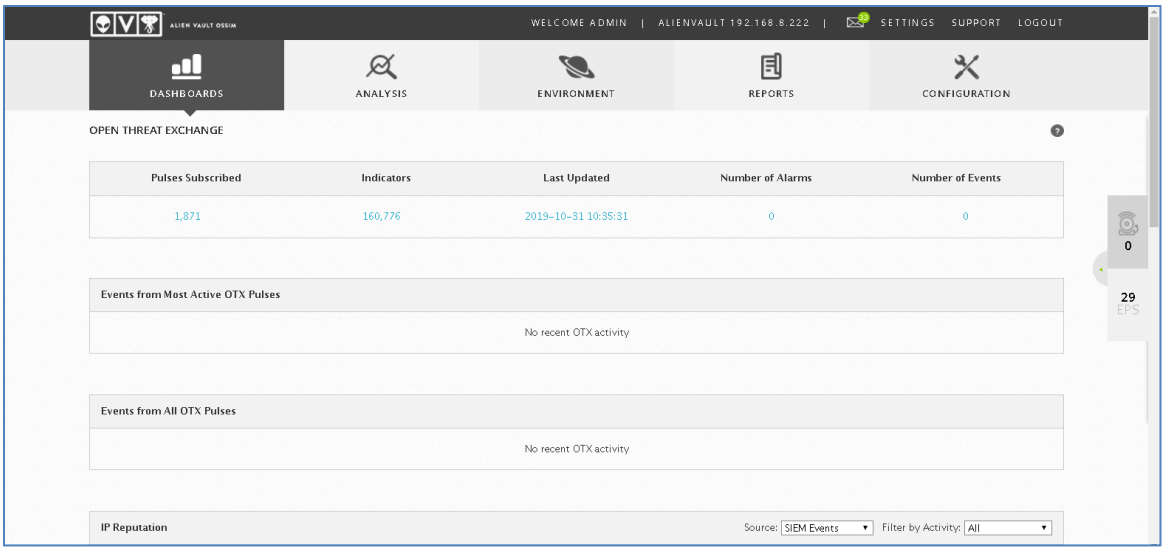


Figura No 81. Cuadro de Mando (Información OTX) (Captura de pantalla de equipo personal)

Dentro de la misma opción explorada en la **Figura No 82** se muestra la reputación a nivel mundial que proporcionan los distintos pulsos de los usuarios donde informan las amenazas o atacantes descubiertos.

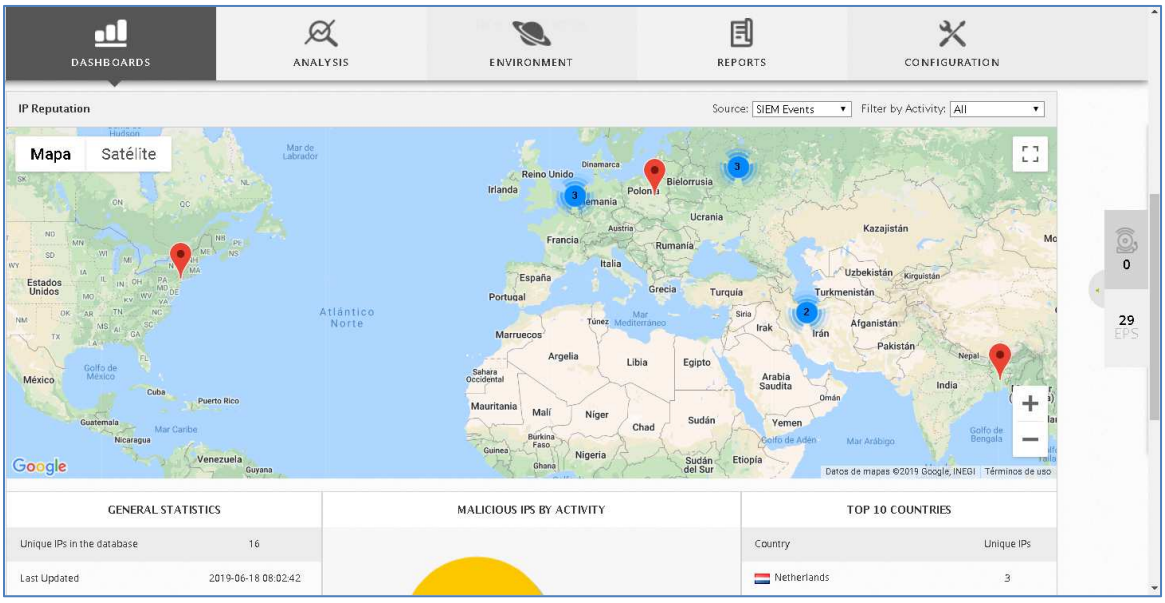


Figura No 82. Ubicación geográfica de atacantes según OTX (Captura de pantalla de equipo personal)

Se puede observar en la **Figura No 83** que los datos de los hallazgos de amenazas que estaban en el mapa ahora tabulado dando más detalle de los países de donde proceden los atacantes.

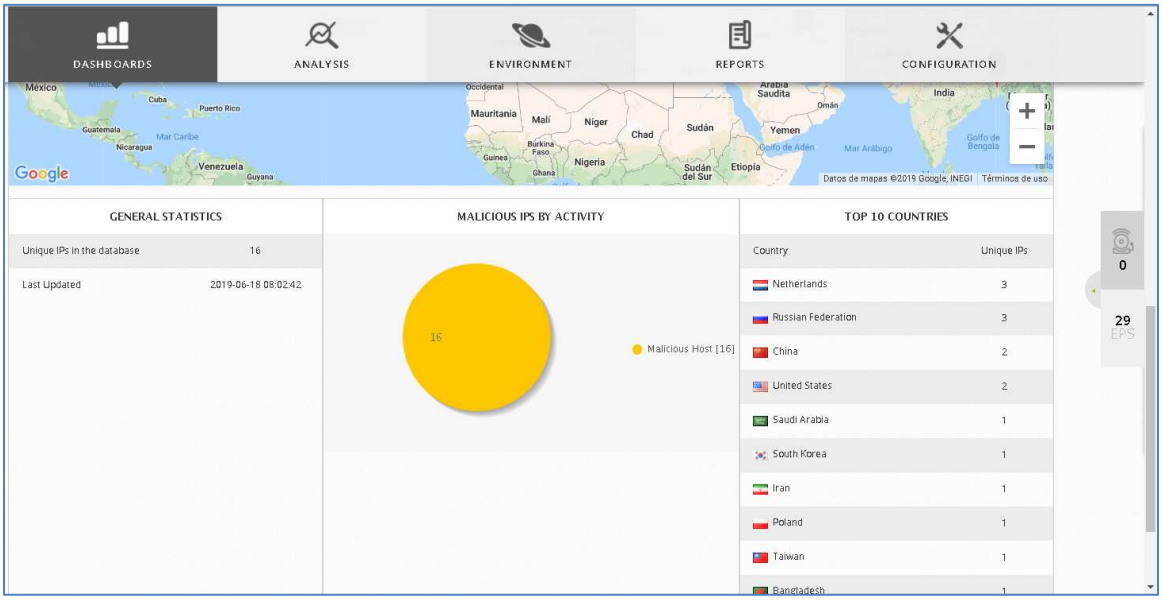


Figura No 83. Tabulación de atacantes del mapa provisto por OTX (Captura de pantalla de equipo personal)

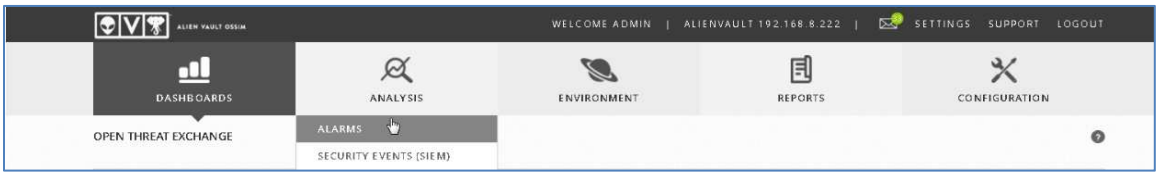


Figura No 84. Sub Menú Alarmas dentro de Análisis (Captura de pantalla de equipo personal)

En el menú ANALYSIS (en español análisis) existen varios sub-menú dentro de los cuales se encuentra ALARMS (en español alarmas), ver **Figura No 84**, que mostrará todas las alarmas detectadas por el SIEM en tiempo real. El SIEM clasifica en varios tipos las alarmas. Estas alarmas son producto de las detecciones automáticas del motor de correlación o por alguna programación que nosotros podamos efectuar. **Ver Figura No 85.**

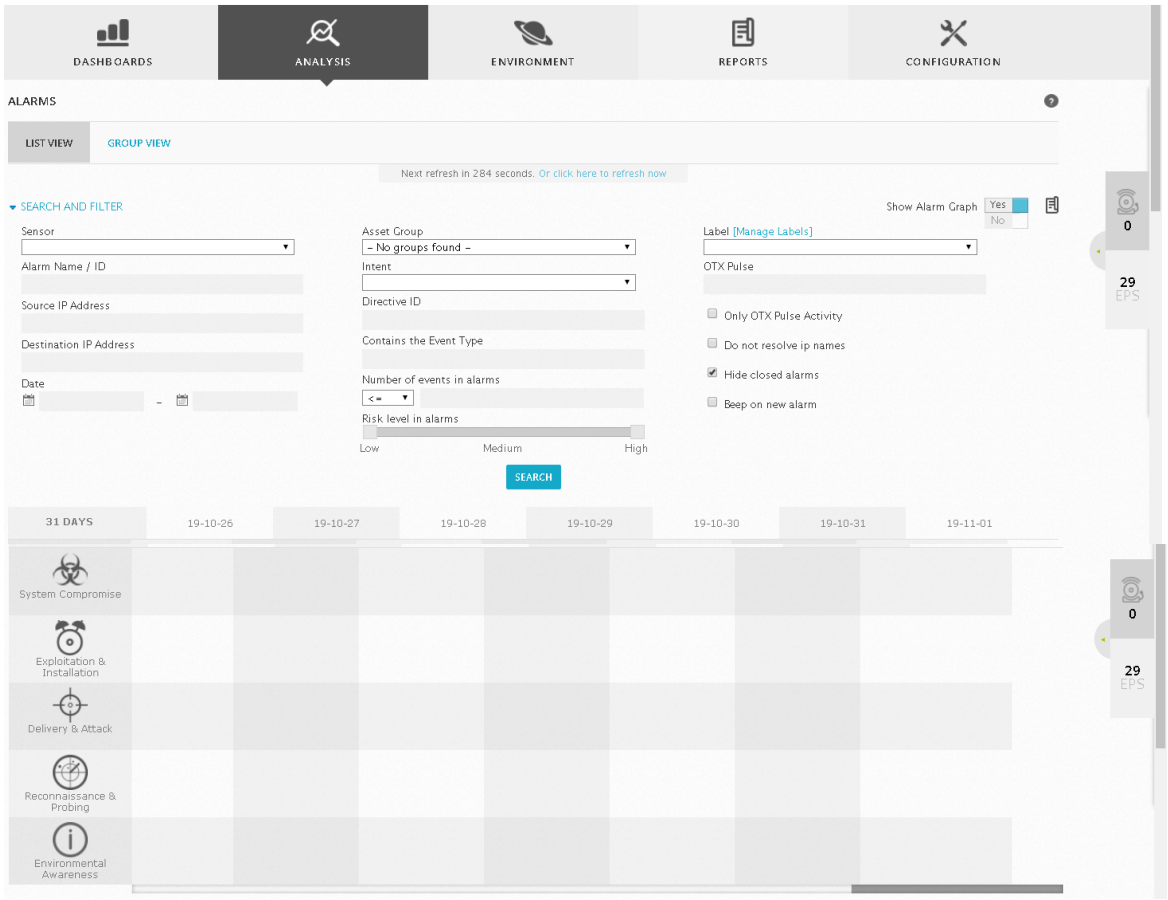


Figura No 85. Informe de Alarmas (Captura de pantalla de equipo personal)**.**

En el menú análisis, **ver Figura No 86**, encontramos también la opción "SECURITY EVENTS (SIEM)", en español eventos de seguridad SIEM. En esta opción podemos realizar búsquedas de lo que ha pasado en horas, días, semanas o el último mes en cuanto eventos de seguridad.

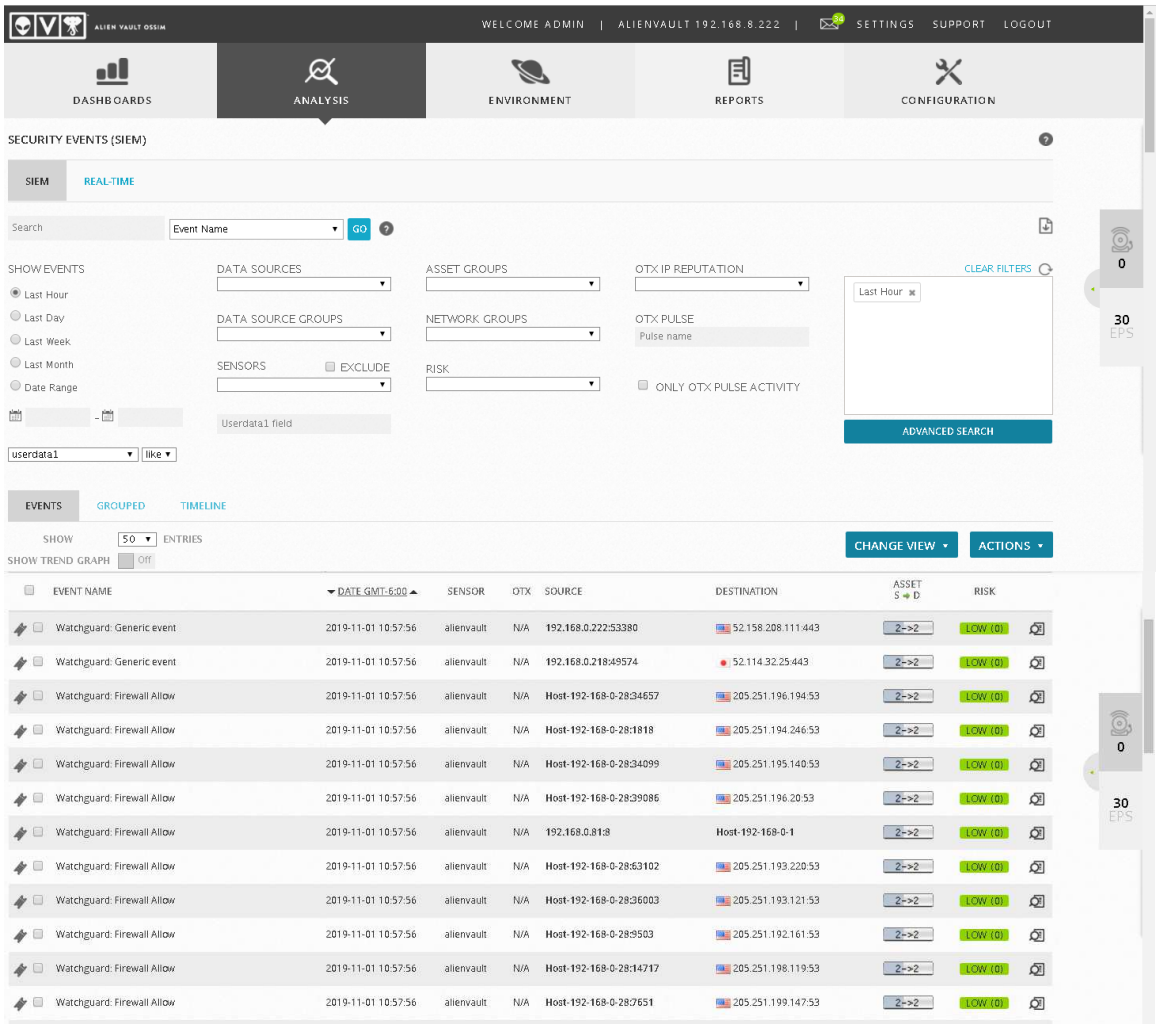


Figura No 86. Eventos de Seguridad - Análisis de SIEM (Captura de pantalla de equipo personal)

En la parte inferior de la **Figura No 56** nos muestra en "EVENT NAME" (en español nombre del evento) la fuente del evento grabado; en este caso el Watchguard. En "SOURCE" (en español fuente) el IP que origina el evento y en "DESTINATION" (en español destino) se muestra el IP destino del evento. Tanto en la fuente como en el destino se muestra el puerto de conexión por cada IP. A la vez se observa en "ASSET" (en español activo) la valoración del activo. En "RISK" (en español riesgo) se muestra el impacto del riesgo registrado.

En la **Figura No 87** de análisis de eventos SIEM también podemos agruparlos en la opción "GRUPED" (en español agrupado). De tal forma el SIEM organiza todos los eventos de seguridad dando un resumen de cada categoría encontrada con su cantidad de eventos. Todo conforme a las fuentes configuradas.

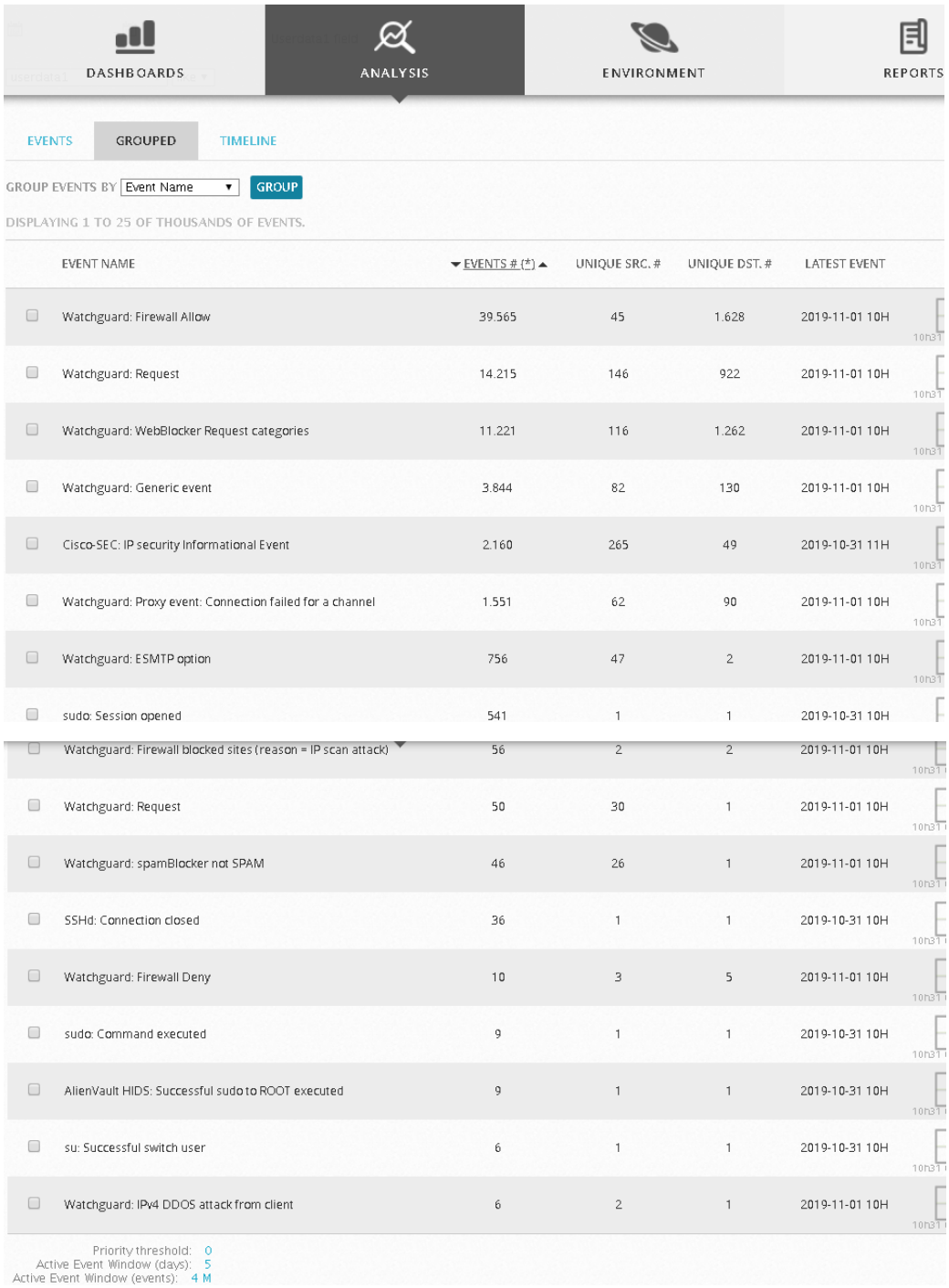


Figura No 87. Eventos de Seguridad Agrupados por Categoría (Captura de pantalla de equipo personal)

En la Clasificación de la **Figura No 87** se puede observar detalles de los eventos por agrupaciones indicando los eventos, cantidad generadas por únicas fuentes y por destinos. En la **Figura No 88** de este detalle del SIEM podemos observar un evento de equipos bloqueados por el firewall del UTM.

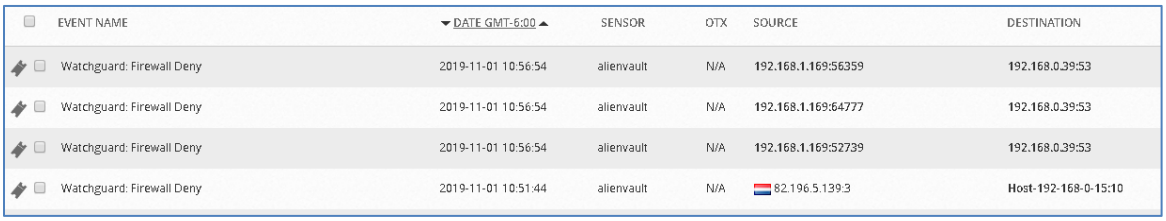


Figura No 88. Selección de Grupo Watchguard: Firewall Deny (Captura de pantalla de equipo personal)

Si hacemos clic sobre alguno de los eventos se puede ver en la **Figura No 89** en detalle la política de bloqueo aplicada por el UTM.

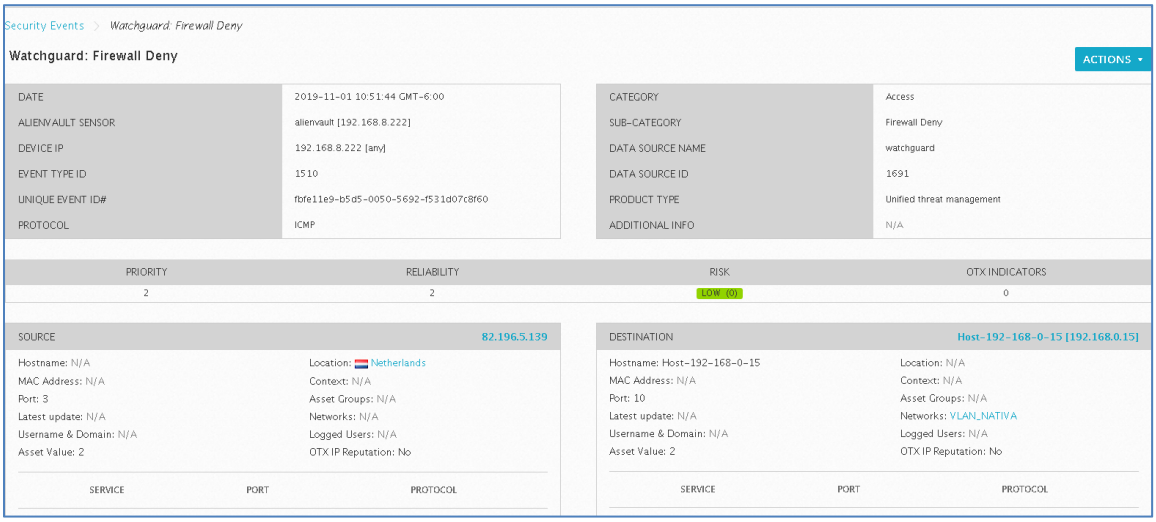


Figura No 89. Detalle de Evento de Grupo Watchguard: Firewall Deny (Captura de pantalla de equipo personal)

Como se observa hay un buen número de categorías que podemos explorar tanto de los eventos almacenados como en tiempo real. De las categorías mostradas en la **Figura No 87** seleccionamos la del ataque de búsqueda de IP ("IP scan attack"). En la **Figura No 90** se observa la lista de bloqueos efectuadas por el UTM. Si se hace clic sobre cualquier evento nos brinda la imagen de la **Figura No 91** donde se observa detalle del atacante (IP, Localización geográfica) y se muestra el puerto bajo ataque en el servidor remoto.

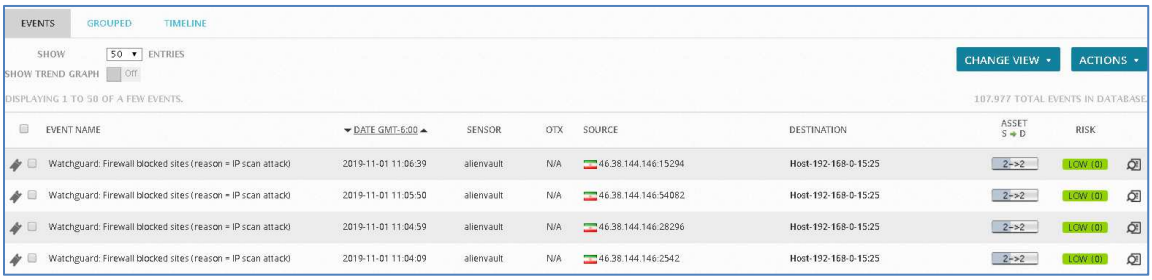


Figura No 90. Lista de Bloqueados por Ataque de escaneo de IP (Captura de pantalla de equipo personal)

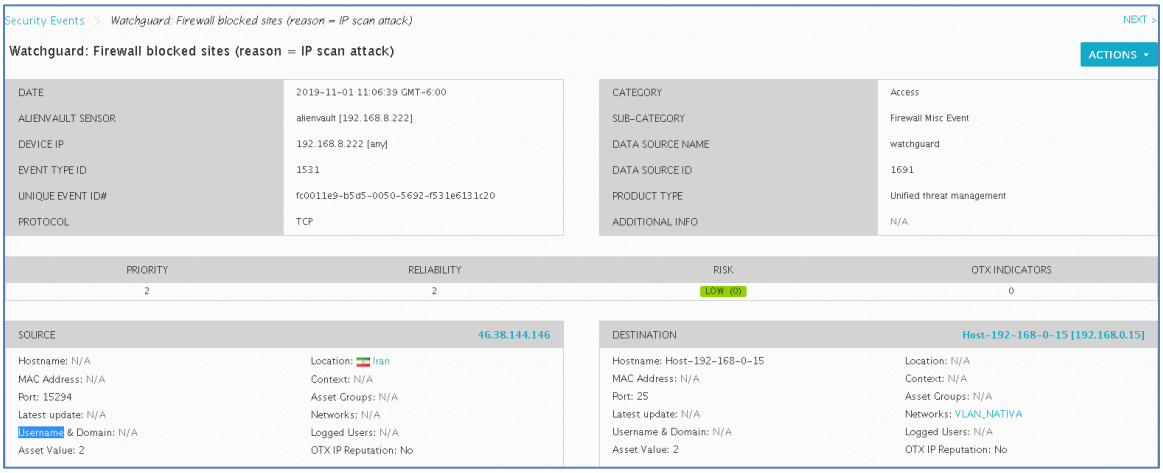


Figura No 91. Detalle de bloqueo por escaneo de IP (Captura de pantalla de equipo personal)

Si seleccionamos de la **Figura No 87** eventos en el grupo de "IPv4 DDOS attack from client" nos muestra la **Figura No 92** con información de los atacante por Denegación de servicios.

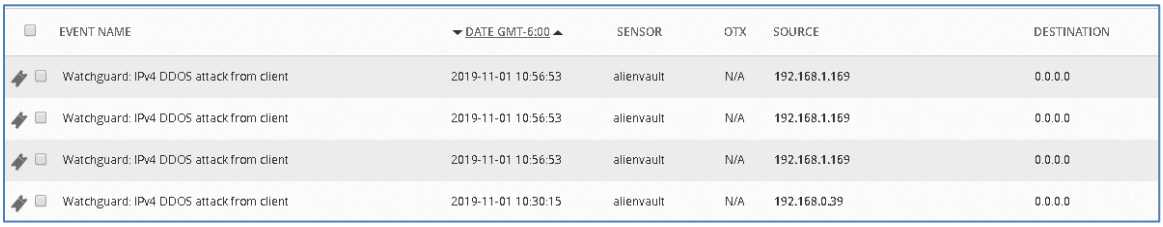


Figura No 92. Atacantes por Denegación de Servicios (Captura de pantalla de equipo personal)

Lo que ahora vamos a realizar es cambiar el idioma del SIEM. Para esto nos vamos al menú "CONFIGURATION" (en español configuración), luego seleccionamos el sub-menú "ADMINISTRATION" (en español administración) y seleccionamos del cuadro combinado que está en la opción "LANGUAGE" (en español idioma) el idioma que deseemos. Ver **Figura No 93**.

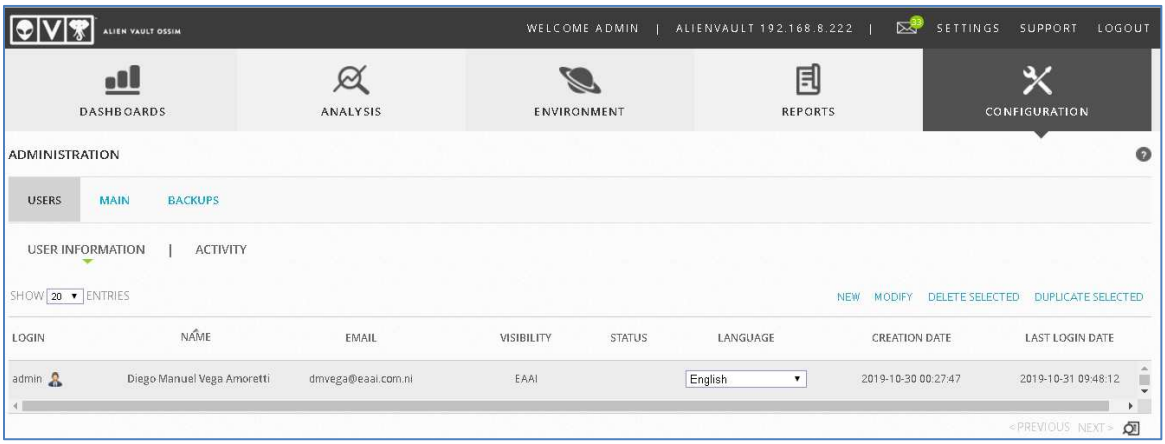


Figura No 93. Cambio de idioma SIEM (Captura de pantalla de equipo personal)

Hemos seleccionado "Español" y de forma inmediata ha cambiado el idioma de la interfaz de OSSIM.

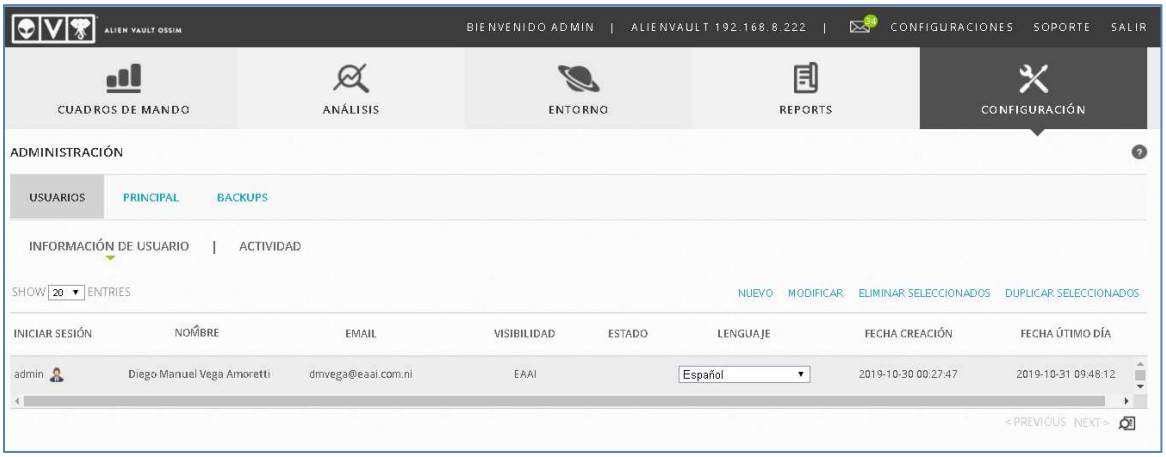


Figura No 94. Idioma de OSSIM en español (Captura de pantalla de equipo personal)

En el SIEM OSSIM encontramos un menú denominado "CONFIGURACIÓN" en el que encontramos ajustes de administración, despliegue, información de amenazas y la opción abrir intercambio de amenazas. En el sub-menú Despliegue encontramos las opciones "COMPONENTES", "PLUGING BUILDER" y "UBICACIONES". El sub-menú "DESPLIEGUE" en su parte de "COMPONENTES" La **Figura No 95** muestra en detalle los componentes del SIEM y su nivel de funcionamiento.

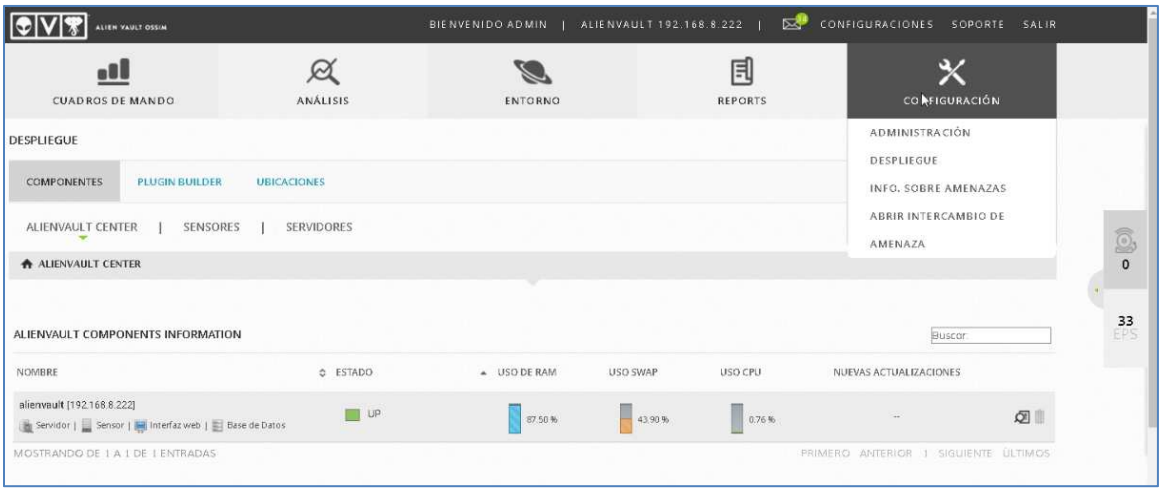


Figura No 95. Estado del Despliegue de OSSIM (Captura de pantalla de equipo personal)

En el sub-menú "ABRIR INTERCAMBIO DE AMENAZA" dentro del menú configuración muestra los pulsos generados a nivel mundial por todos los usuarios de OSSIM. En este caso podemos observar un **exploit de día 0**; que es una vulnerabilidad nueva detectada y explotada. En este caso exploit está relacionado con el "google chrome".

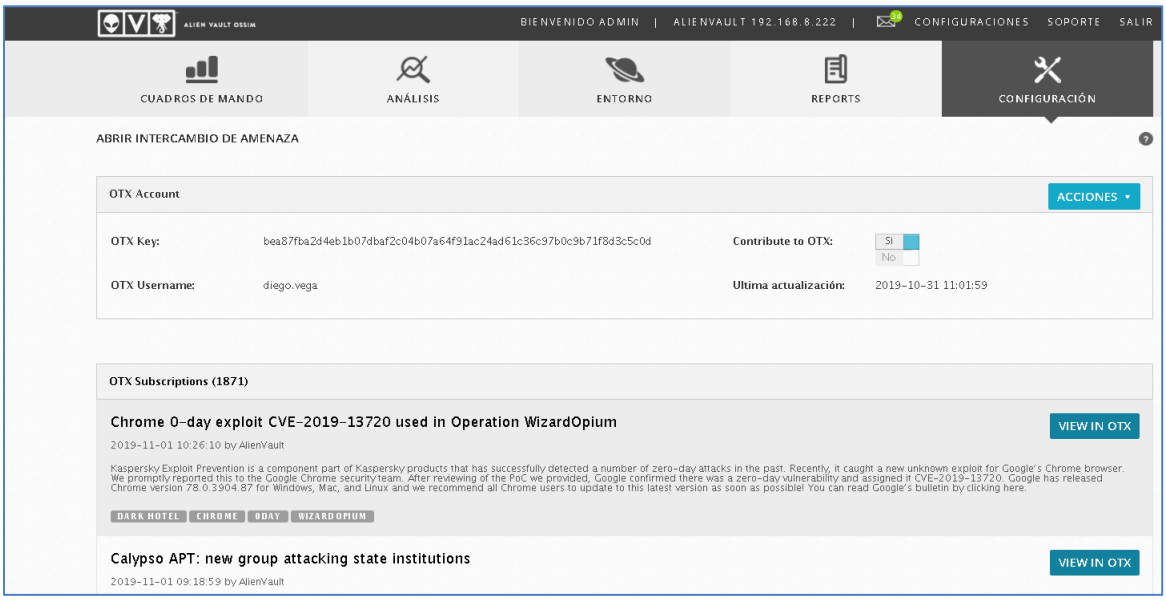


Figura No 96. Información de Intercambio de Amenazas (Captura de pantalla de equipo personal)

Al hacer clic en el pulso del "**exploit**" mostrado en la **Figura No 96** se puede observar en detalle la información. Es importante siempre con la información del CVE (siglas de Common Vulnerabilities and Exposures, en español Vulnerabilidades y exposiciones comunes) brindada por el pulso realizar

comprobación en otros sitios. En este caso nos indica que el **google chrome** ya ha sacado una actualización para evitar la vulnerabilidad detecta.

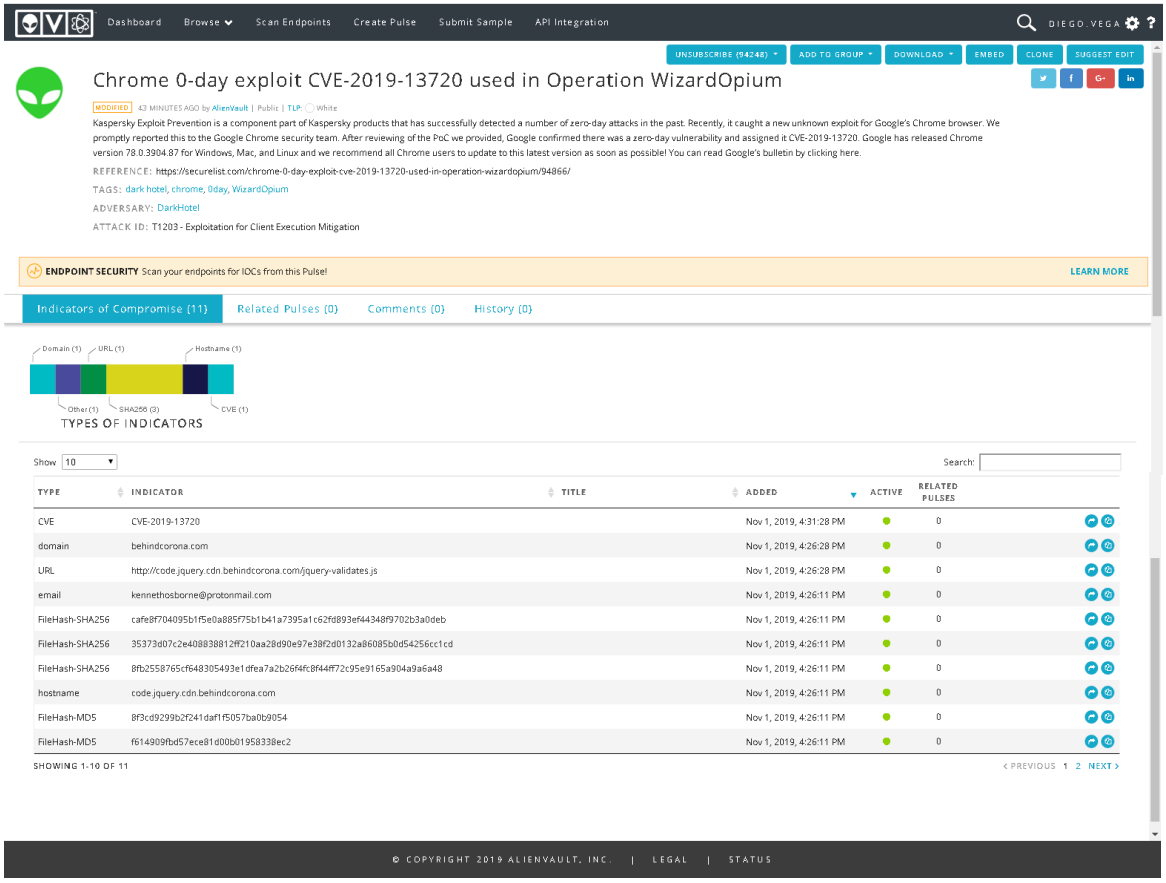


Figura No 97. Información detallada del Exploit (Captura de pantalla de equipo personal)

Así como el pulso mostrado en la **Figura No 97** hay muchos más que son mostrados gracias a nuestra suscripción gratuita. La idea el OTX es establecer una comunidad en la que todos los usuarios del SIEM OSSIM puedan intercambiar información de atacantes y tomar medidas preventivas.

8.5. INTEGRACIÓN DE SENSORES

Para la integración de los sensores que son en realidad los equipos de propósito especial como servidores de correos, DNS, base de datos, antivirus, aplicaciones o cualquier otro tipo de equipo con propósito definido se debe hacer lo siguiente. Seleccionar un activo como en nuestro caso un equipo con Windows 2016. Este equipo que seleccionamos es uno de los que falló el despliegue del asistente inicial de OSSIM. En el sistema de archivos del equipo localizamos el archivo llamado "**ossec-win32-agent.exe**" y lo ejecutamos como se muestra en la **Figura No 98**. El error inicial en el paso 4 del asistente fue que las credenciales que usamos aunque son de administrador a nivel del Windows no se permiten la ejecución remota de aplicaciones y el OSSIM solo puede completar la tarea de copiar el ejecutable del HIDS pero no puede instalarlo.

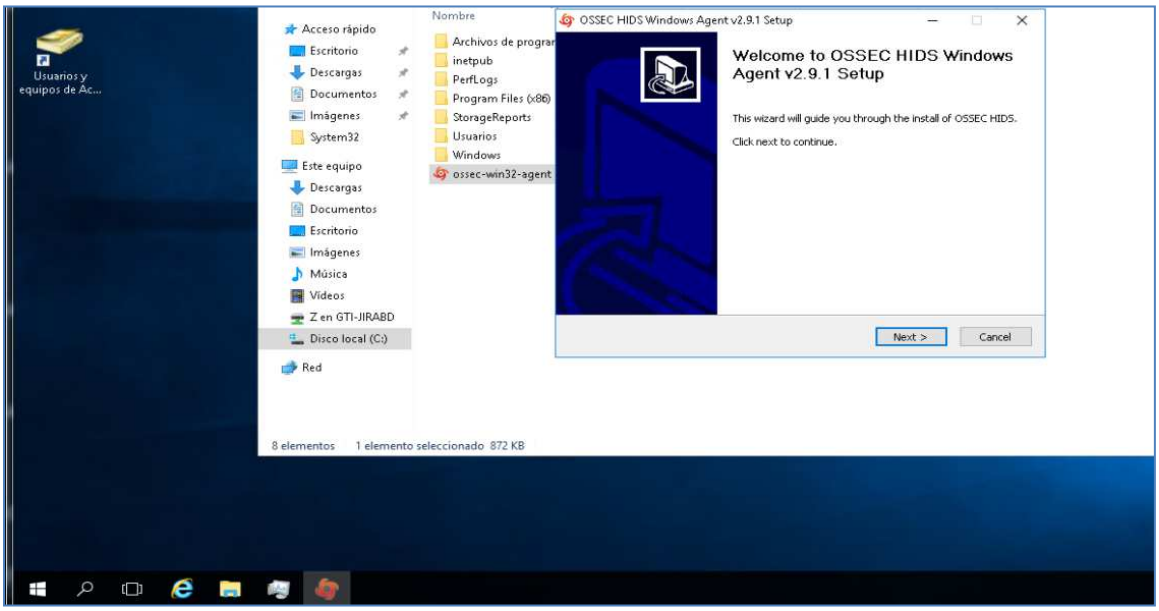


Figura No 98 Instalación de HIDS OSSEC en Windows (Captura de pantalla de equipo personal)

Ahora solo hacemos clic en "Next" (en español siguiente) para continuar el instalador. Lo que hacemos en la **Figura No 99** es hacer clic en "I Agree" (en español yo acepto) para aceptar el contrato de la licencia de uso del software gratuito.

Figura No 99. Aceptando Licencia de OSSEC(Captura de pantalla de equipo personal)

Luego en la **Figura No 100** seleccionamos todos los componentes del HIDS. El primero es el agente como tal. Luego el componente de los LOG y el de chequeo de integridad. Clic en "Next" (en español siguiente)

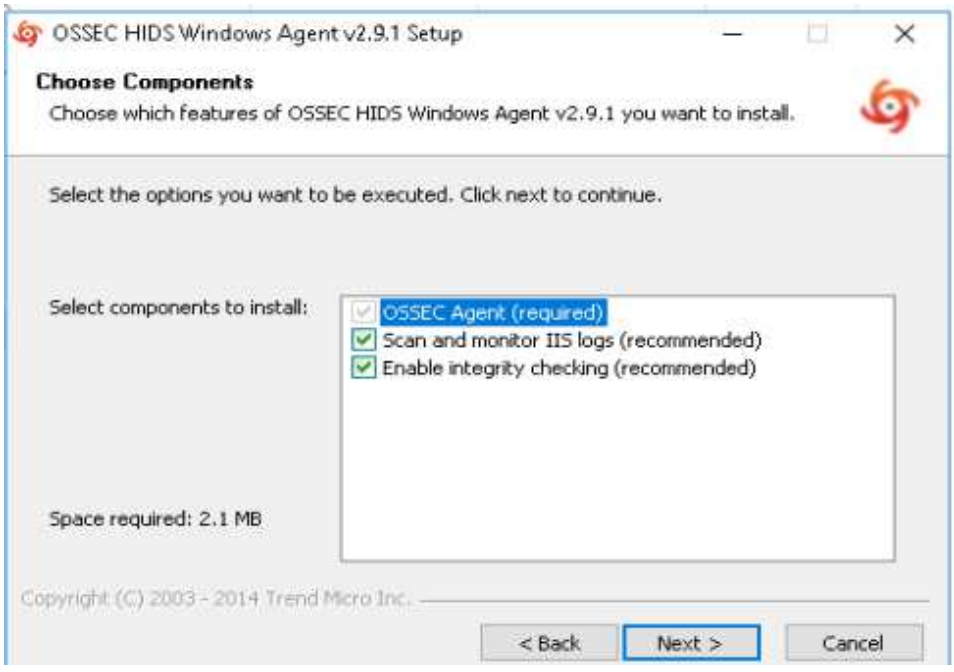


Figura No 100. Componentes del HIDS OSSEC (Captura de pantalla de equipo personal)

En la **Figura No 101** se muestra la finalización del instalar y clic en "Finish" (en español finalizar) para concluir la instalación.

Figura No 101. Finalizando Instalación de HIDS OSSEC (Captura de pantalla de equipo personal)

La **Figura No 102** muestra la configuración del agento con el IP del OSSIM y la clave cifrada para establecer comunicación.

Figura No 102. Configuración de agente OSSEC (Captura de pantalla de equipo personal)

Con los datos obtenidos del OSSIM damos clic en "Save" (Salvar en español), ver **Figura No 102**. Luego se realiza un proceso de verificación de datos al cual solo le hacemos clic en "Aceptar". Con los datos ya guardados solo restar arrancar el agente. En el menú "Manage" haciendo clic en "Start OSSEC" (en español Iniciar OSSEC).

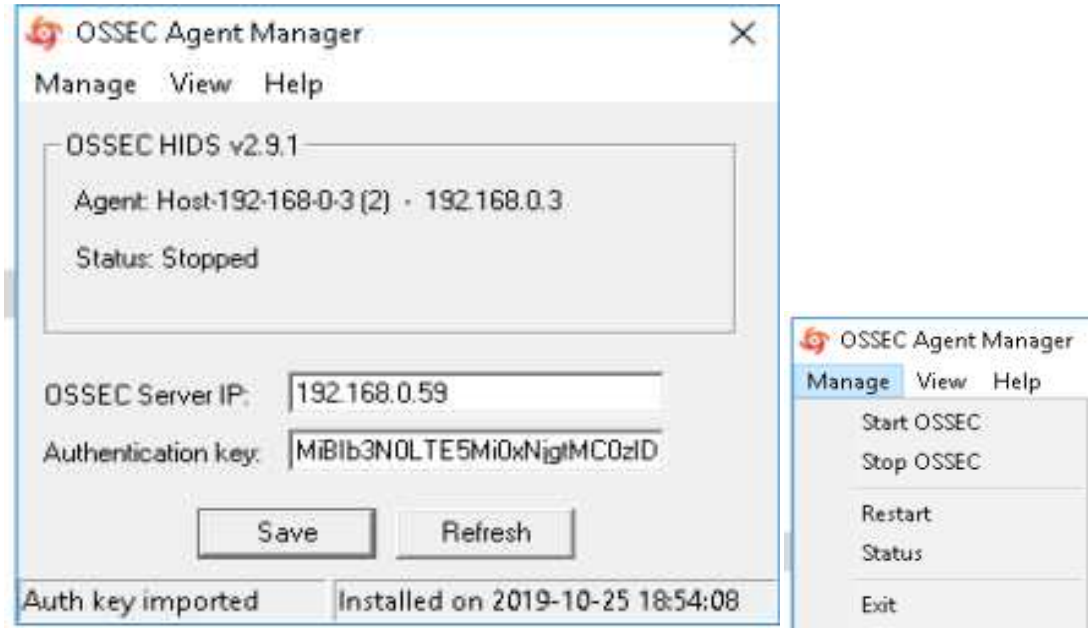


Figura No 103. Iniciando Agente OSSEC (Captura de pantalla de equipo personal)

En la Figura No 104 se muestra el agente de OSSEC ya está inicializado sin problemas.

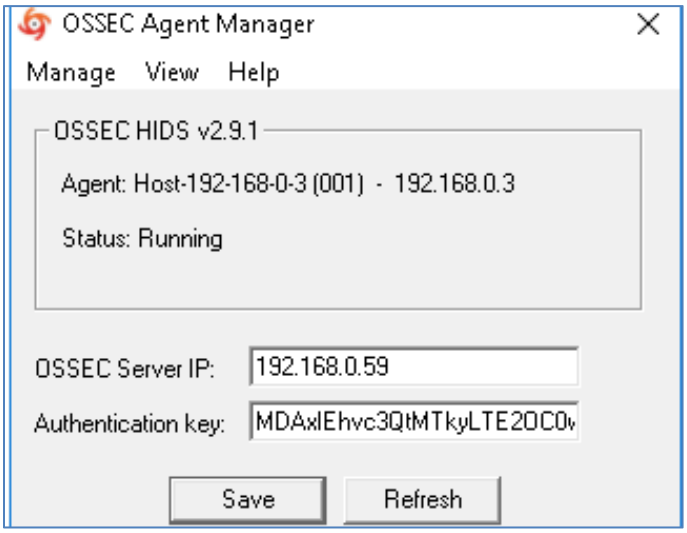


Figura No 104. Agente OSSEC Iniciado (Captura de pantalla de equipo personal)

El proceso de instalación descrito con anterioridad se hizo en paralelo con el del equipo Windows 7 que también había fallado el paso 4. Lo que ahora se mostrará es el lugar de donde se obtuvo la clave de autenticación mostrada en la **Figura No 102** para el agente del equipo Windows 2016. Como se observa ya está activo el equipo con Windows 7, ahora para activar el Windows 2016 copiamos la clave obtenida en la **Figura No 105** al hacer clic en el icono de la llave. Se nota que el ID de la llave es el 001 para el equipo en mención.

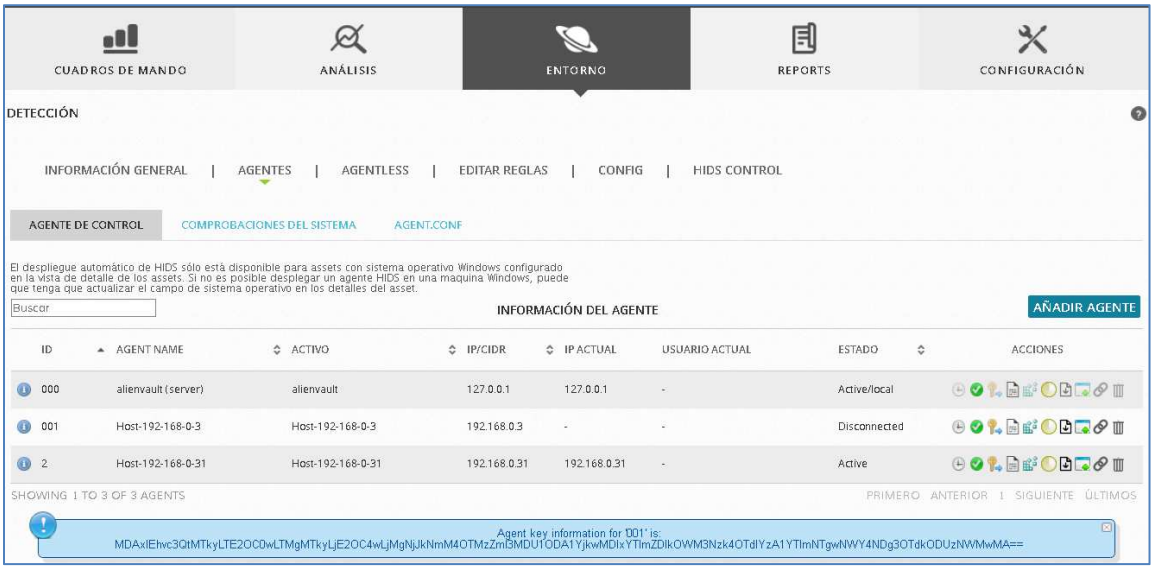


Figura No 105. Obteniendo Clave de Agente OSSEC (Captura de pantalla de equipo personal)

Una vez que los dos agentes están activos en ambos equipos podemos observar que las conexiones al OSSIM están perfectas, tal como se muestra en La **Figura No 106**. En algunos casos es necesario hacer clic en el icono del reloj para reiniciar el servicio en el OSSIM. Si no conecta de forma inmediata un reinicio del OSSIM resuelve el problema de refrescamiento de la interfaz.

Figura No 106. Agentes OSSEC Activos (Captura de pantalla de equipo personal)

Hasta el momento los equipos que hemos integrado son Windows. En el caso de Linux al inicio del asistente de OSSIM dio la impresión que ya estaba instalado y activo perfectamente. Pero en realidad se instaló de una forma más limitada. Si se observa en la **Figura No 107** no está en la lista de agentes y en el asistente inicial no presentó problemas. Pero si está en la opción de "DETECCION" en "AGENTLESS"; sub-menú de "ENTORNO".

Figura No 107. HIDS en modo sin agente (Captura de pantalla de equipo personal)**.**

Por lo expuesto anteriormente es necesario realizar pasos adicionales que incurren en una configuración más avanzada del agente bajo Linux. Para poder llevar a cabo la instalación se debe hacer una personalización a la instalación de OSSIM. Lo continúa describen todo el proceso.

Lo primero que se muestra en la **Figura No 108** es una conexión vía SSH al servidor OSSIM. Una vez introducida la clave del usuario "root" inicia la carga inmediata del menú de instalación del OSSIM. Si observamos en la imagen de abajo el Linux que correo en OSSIM es un debían 4.9.168-1

Figura No 108. Conexión SSH a OSSIM (Captura de pantalla de equipo personal)

Luego que logramos la conexión la **Figura No 109** muestra el menú de las opciones del instalador de AlienVault OSSIM. La opción que nos interesa es "Jailbreak System" (**Jailbreak** es una palabra compuesta que en español significa un escape de la cárcel), para nosotros liberación del sistema y sus reglas. Con el jailbreak obtenemos un **Shell** del sistema OSSIM con poder de "root" para hacer lo que deseemos. Esta opción no solo es peligrosa porque

podes dañar el sistema; también es para usuario avanzados que sepan como personalizar opciones que OSSIM normalmente no permite. Como es el caso de la instalación completa de un agente bajo Linux.

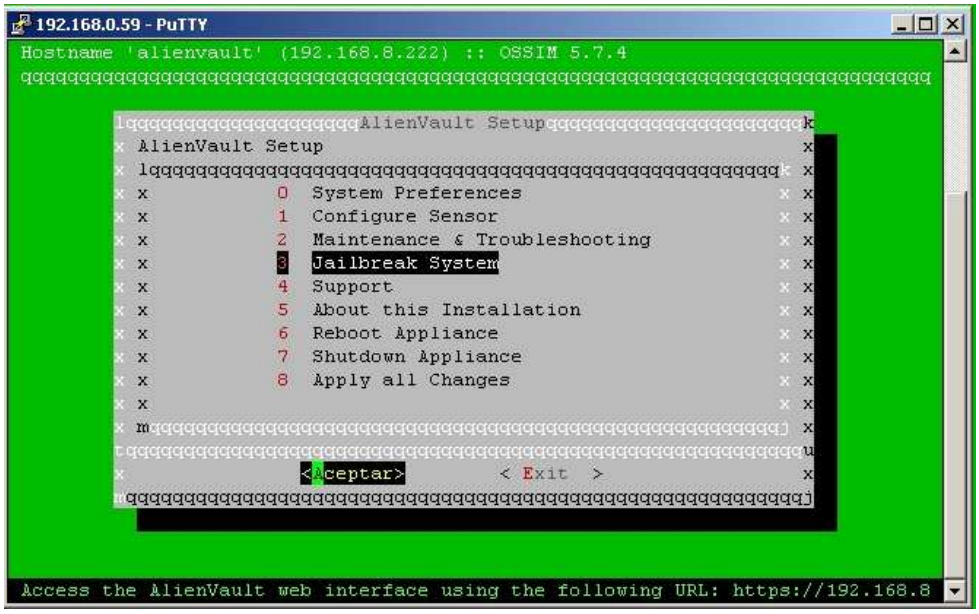


Figura No 109. Menú OSSIM en conexión SSH (Captura de pantalla de equipo personal)

Después de seleccionar la opción 3 hacer clic en "Aceptar".

En el sitio de AlienVault https://www.alienvault.com/documentation/usm-appliance/system-overview/unauthorized-modification.htm nos dicen que no debemos hacer modificación a las configuraciones internas del sistema OSSIM o USM. Al hacer clic en Aceptar de la pantalla del instalador de OSSIM vía SSH en la opción 3 nos activa otra ventana mostrada en la Figura No 110 que nos pregunta si deseamos continuar. Nos advierte que vamos a obtener acceso completo a la línea de comandos.

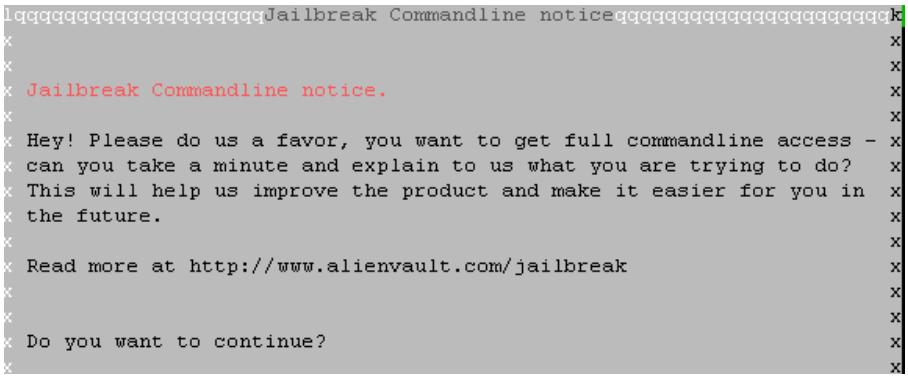


Figura No 110. Acceso a consola en modo ROOT (Captura de pantalla de equipo personal)

Seleccionamos "S?" y luego nos muestra el SHELL. Lo que hacemos con la línea de comandos es ir a la ubicación del administrador del agente de OSSIM. Este está en la ruta /var/ossec/bin. Luego ejecutamos el archivo "manage_agents". Escribimos "A" para agregar un agente de forma manual. Ver **Figura No 111**.

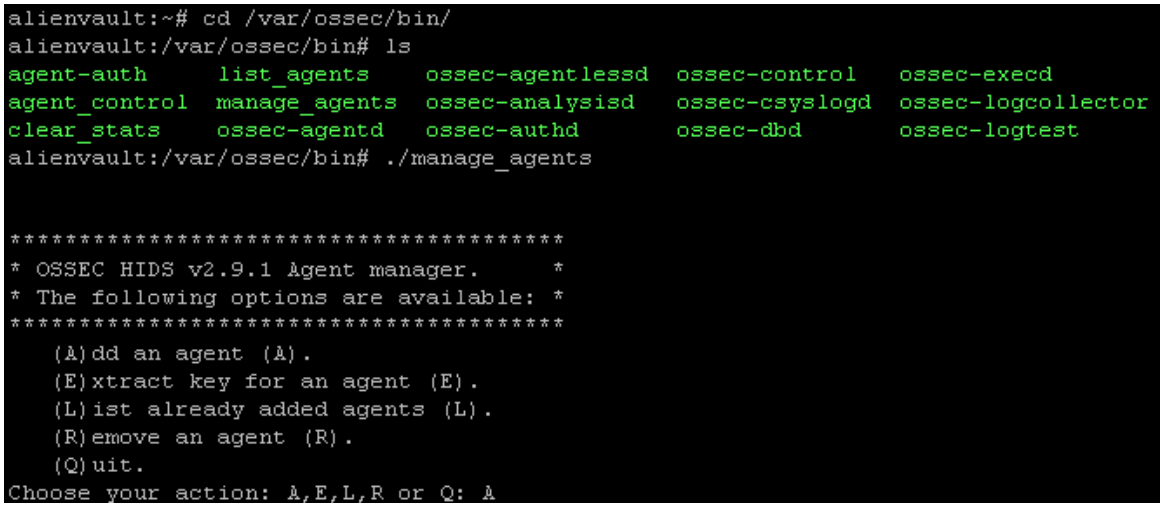


Figura No 111. Administrador de OSSEC vía SSH (Captura de pantalla de equipo personal)

Luego nos comienza a preguntar nombre del agente ("A name for the new agent"), escribimos CentosOs7-LogServer. Después de ese dato pregunta la dirección IP del agente ("The IP Address of the new agent") de lo cual escribimos 192.168.0.118.Finalmente en la **Figura No 112** nos pregunta el ID del nuevo agente ("An ID for the new agent [002]"), por defecto tenía 002; pero como ya tenemos los ID 001, 2 no es conveniente usar el 002 y escribimos 003.

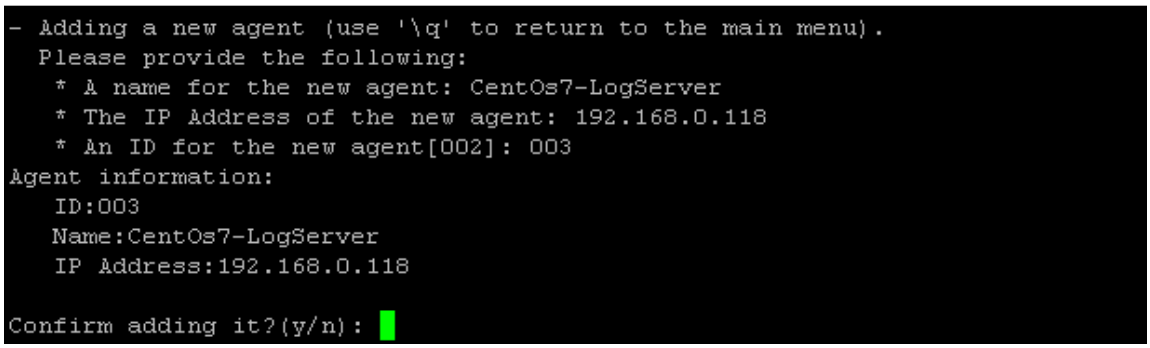


Figura No 112. Creación de Agente para Centos7-Log Server (Captura de pantalla de equipo personal)

A la pregunta de confirmación de escribimos "y".

Ahora con el agente ya creado sólo escribimos la opción "E" para extraer la clave. Tal como se muestra en la **Figura No 113**. Con la opción **E** ya activada

nos pregunta de qué agente debemos extraer la clave. En este caso seleccionamos (Provide the ID of the agent to extract the key) escribimos el ID "**003**".

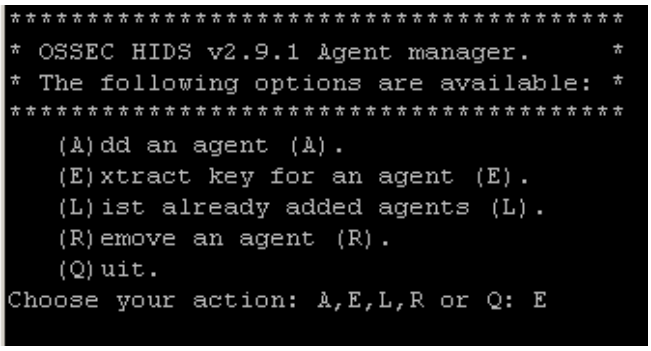


Figura No 113. Selección de opción para extraer clave de OSSEC (Captura de pantalla de equipo personal)

En la **Figura No 114** se muestra la clave generada para el ID 003.

Figura No 114. Clave generada para agente de OSSEC (Captura de pantalla de equipo personal)

Luego seleccionamos la cadena de texto generada que son datos cifrados y la pegamos en el block de notas para luego usarla en el agente de Linux del servidor de LOG. Tal como se muestra en la **Figura No 115**.

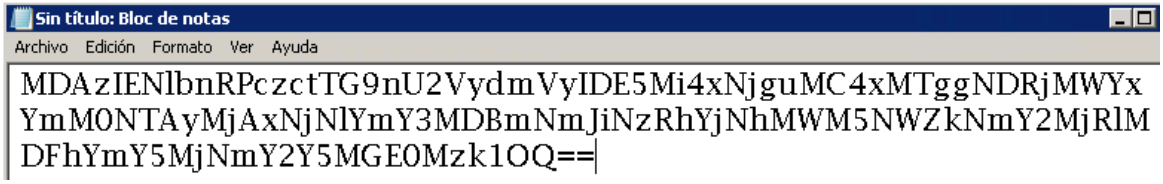


Figura No 115. Llave copiada en block de notas

Ahora empezamos a instalar 3 componentes indispensables para instalar el agente OSSEC en Linux. Estos son:

- Repositorio epel versión 6.8
- Repositorio remi versión 6
- atomic

Lo primero que se muestra es la **Figura No 116** en la que se establece conexión SSH al servidor de LOG. Luego se prueba con wget bajando e instalando directamente el repositorio de epel requerido.

Figura No 116. Instalado repositorio de EPEL (Captura de pantalla de equipo personal)

Figura No 117. Instalación de paquete remi (Captura de pantalla de equipo personal)

En la **Figura No 117** se ha instalado satisfactoriamente el paquete remi. Solo falta el componente de atomic. Empleamos la línea de comandos de la Figura No 117:

```
wget -q -O - http://www.atomicorp.com/installers/atomic | sh
```

```
[root@logserver-aimacs-com-ni ~]# wget -q -O - http://www.atomicorp.com/installers/atomic | sh
[root@logserver-aimacs-com-ni ~]# wget -q -O - http://www.atomicorp.com/installers/atomic
[root@logserver-aimacs-com-ni ~]# wget -q -O - http://www.atomicorp.com/installers/atomic | sh
[root@logserver-aimacs-com-ni ~]#
```

Figura No 118. Comando1 para instalar atomic (Captura de pantalla de equipo personal)

Como no funciona se descarga el contenido del archivo atomic y se guarda en Linux con el nombre "atomic.sh". Una vez guardado solo lo ejecutamos con ./atomic.sh en la localidad que lo guardamos, tal como lo muestra la **Figura No 119**. En este caso el root de la unidad (/).

```
[root@logserver-aimacs-com-ni ~]# bash atomic.sh

Atomic Free Unsupported Archive installer, version 5.0

BY INSTALLING THIS SOFTWARE AND BY USING ANY AND ALL SOFTWARE
PROVIDED BY ATOMICORP LIMITED YOU ACKNOWLEDGE AND AGREE:

THIS SOFTWARE AND ALL SOFTWARE PROVIDED IN THIS REPOSITORY IS
PROVIDED BY ATOMICORP LIMITED AS IS, IS UNSUPPORTED AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL ATOMICORP LIMITED, THE
COPYRIGHT OWNER OR ANY CONTRIBUTOR TO ANY AND ALL SOFTWARE PROVIDED
BY OR PUBLISHED IN THIS REPOSITORY BE LIABLE FOR ANY DIRECT,
INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
OF THE POSSIBILITY OF SUCH DAMAGE.

For supported software packages please contact us at:

  sales@atomicorp.com

Do you agree to these terms? (yes/no) [Default: yes] yes

Configuring the [atomic] repo archive for this system

Installing the Atomic GPG keys: OK
```

Figura No 119. Ejecución de instalador de atomic (Captura de pantalla de equipo personal)

En la **Figura No 119** contestamos a las preguntas de aceptar los términos "YES" y a la de Instalar claves GPG de atomic "OK".

```
Downloading atomic-release-1.0-21.el7.art.noarch.rpm: warning: atomic-release-1.0-21.el7.art.noarch.rpm: Header V4 RSA/SHA256 Signature,
Preparing...                          ################################# [100%]
Updating / installing...
   1:atomic-release-1.0-21.el7.art    ################################# [100%]
OK

Enable repo by default? (yes/no) [Default: yes]: yes


The Atomic repo has now been installed and configured for your system
The following channels are available:
  atomic          - [ACTIVATED] - contains the stable tree of ART packages
  atomic-testing  - [DISABLED]  - contains the testing tree of ART packages
  atomic-bleeding - [DISABLED]  - contains the development tree of ART packages
```

Figura No 120. Atomic instalado

Luego se descarga la versión de **atomic-release-1.0-21.el7.art.noarch.rpm**; se observa en la **Figura No 120** que atomic ya está activo. Ahora con todos los requisitos ya completados solo nos queda instalar el agente, para esto lo descargamos usando el yum. Inicialmente buscamos el paquete ossec-hids-client

```
yum install ossec-hids-client
```

En nuestro caso fallo y buscamos un paquete alternativo que es **ossec-hids-agent.x86_64.** En la **Figura No 121** se muestra el proceso de instalación del agente OSSEC..

```
[root@logserver-aimacs-com-ni ~]# yum install ossec-hids-agent.x86_64
Complementos cargados:fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * atomic: www7.atomicorp.com
 * base: mirror.atlantic.net
 * epel: sjc.edge.kernel.org
 * extras: bay.uchicago.edu
 * nux-dextop: li.nux.ro
 * updates: mirror.den1.denvercolo.net
Resolviendo dependencias
--> Ejecutando prueba de transacción
---> Paquete ossec-hids-agent.x86_64 1:3.4.0-9229.el7.art debe ser instalado
--> Procesando dependencias: ossec-hids = 1:3.4.0-9229.el7.art para el paquete: 1:ossec-hids-agent-3.4.0-9229.el7.art.x86_64
--> Ejecutando prueba de transacción
---> Paquete ossec-hids.x86_64 1:3.4.0-9229.el7.art debe ser instalado
--> Resolución de dependencias finalizada
```

Figura No 121. Instalación de agente OSSEC en Centos7-Log Server(Captura de pantalla de equipo personal)

Se bajan las dependencias requeridas del paquete.

```
advertencia:/var/cache/yum/x86_64/7/atomic/packages/ossec-hids-3.4.0-9229.el7.art.x86_64.rpm: EncabezadoV4 RSA/SHA256 
No se ha instalado la llave pública de ossec-hids-3.4.0-9229.el7.art.x86_64.rpm
(1/2): ossec-hids-3.4.0-9229.el7.art.x86_64.rpm
(2/2): ossec-hids-agent-3.4.0-9229.el7.art.x86_64.rpm
--------------------------------------------------------------------------------------------------------------------------------
Total
Obteniendo clave desde file:///etc/pki/rpm-gpg/RPM-GPG-KEY.art.txt
Importando llave GPG 0x5EBD2744:
 Usuarioid  : "Atomic Rocket Turtle <admin@atomicrocketturtle.com>"
 Huella     : 292e b92e f0e0 77e4 19c6 daff 32a9 5114 5ebd 2744
 Paquete    : atomic-release-1.0-21.el7.art.noarch (installed)
 Desde      : /etc/pki/rpm-gpg/RPM-GPG-KEY.art.txt
Está de acuerdo [s/N]:
```

Figura No 122. Descarga de dependencias (Captura de pantalla de equipo personal)**.**

En la **Figura No 122** luego de bajar las dependencias nos pregunta si queremos descargar un archivo de clave y le decimos que si. Escribimos "S".

```
Está de acuerdo [s/N]:s
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Advertencia: Las bases de datos (RPMDB) han sido modificadas por un elemento ajeno a yum.
  Instalando     : 1:ossec-hids-3.4.0-9229.el7.art.x86_64
  Instalando     : 1:ossec-hids-agent-3.4.0-9229.el7.art.x86_64
  Comprobando    : 1:ossec-hids-agent-3.4.0-9229.el7.art.x86_64
  Comprobando    : 1:ossec-hids-3.4.0-9229.el7.art.x86_64

Instalado:
  ossec-hids-agent.x86_64 1:3.4.0-9229.el7.art

Dependencia(s) instalada(s):
  ossec-hids.x86_64 1:3.4.0-9229.el7.art

¡Listo!
[root@logserver-aimacs-com-ni ~]#
```

Figura No 123. Finalización de Instalación de OSSEC (Captura de pantalla de equipo personal)

La **Figura No 123** muestra que todo está instalado. Solo falta inicializar el agente. Hay que ir a la carpeta /var/ossec/bin y localizar el archivo "ossec-control" y lo ejecutamos con la opción "start" tal como se muestra en la **Figura No 124**.

```
root@logserver-aimacs-com-ni:/var/ossec/bin
[root@logserver-aimacs-com-ni bin]# ./ossec-control  start
Starting OSSEC HIDS 3.4.0...
Started ossec-execd...
2019/11/01 08:18:53 ossec-agentd: INFO: Using notify time: 600 and max time to r
econnect: 1800
2019/11/01 08:18:53 going daemon
Started ossec-agentd...
2019/11/01 08:18:53 ossec-logcollector: Remote commands are not accepted from th
e manager. Ignoring it on the agent.conf
2019/11/01 08:18:53 ossec-logcollector(1202): ERROR: Configuration error at '/va
r/ossec/etc/shared/agent.conf'. Exiting.
Started ossec-logcollector...
2019/11/01 08:18:53 ossec-syscheckd(1756): ERROR: Duplicated directory given: '/
etc'.
2019/11/01 08:18:53 ossec-syscheckd(1756): ERROR: Duplicated directory given: '/
bin'.
Started ossec-syscheckd...
Completed.
```

Figura No 124. Arranca de agente OSSEC. (Captura de pantalla de equipo personal)

Estos errores son producto de que al inicio habíamos intentado instalar el agente pero no fue completo. Ahora comprobamos el estado del servicio del agente con el comando "./ossec-control status".

Como se puede observar en la **Figura No 125** la instalación fue exitosa. Ahora hay que configurar el agente con todas sus opciones.

Figura No 125. Estado de OSSEC (Captura de pantalla de equipo personal)

Siempre en el directorio bin localizamos el archivo ossec-configure para iniciar la configuración del agente. Una vez que ejecutamos el archivo con el comando "./ossec-configure". Una vez ejecutado se nos muestran una serie de preguntas en la **Figura No 126**. La pregunta inicial dice: ¿ Desea una dirección de notificación? luego escribimos la dirección de correos dmvega@eaai.com.ni y el IP del servidor de correos temporal 192.168.0.18. Cuando hemos llenado los datos de notificación nos pregunta si queremos chequeo de integridad, detección de rootkit (traducido muchas veces como encubridor es una palabra compuesta de root y kit, términos para administrador de Linux y conjunto de herramientas) o algún software malicioso oculto para acceso con privilegios, respuesta activa y firewall para bloqueos y contestamos a todas esas preguntas que **SI** con la letra "Y".

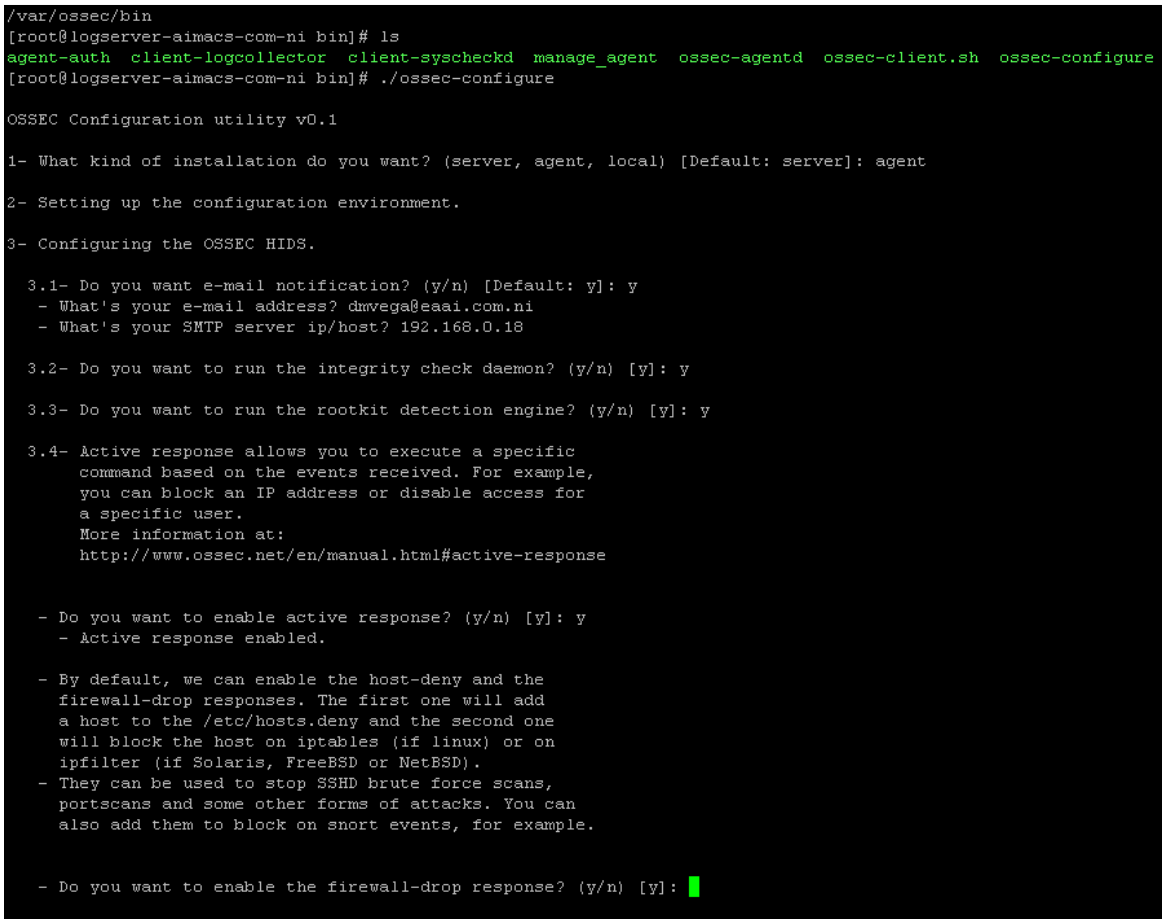


Figura No 126. Configuración de agente OSSEC en Linux.

El firewall con respuesta de bloqueo automática requiere como paso posterior llenar un listado de IP de confianza.

Le damos el listado de IPs de confianza que sería nuestra lista blanca. Estos IPs siempre tendrán acceso al equipo sin importar que pase o que se detecte. **Ver Figura No 127**.

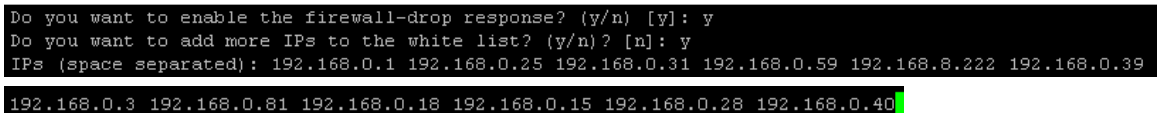


Figura No 127. Lista Blanca para OSSEC (Captura de pantalla de equipo personal)

Ahora en la **Figura No 128** nos pregunta si deseamos activar syslog. Respondemos: "Y" y con eso finalizamos las configuraciones. Pero aun hay que hacer un cambio para indicar el IP del servidor de OSSIM.

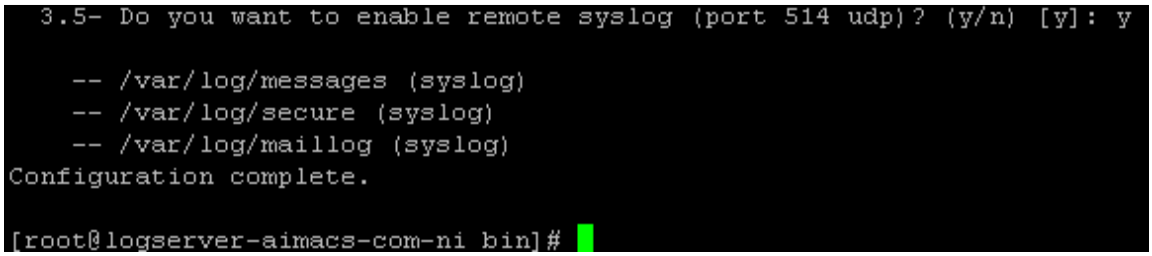


Figura No 128. Activación de Syslog en OSSEC (Captura de pantalla de equipo personal)

El archivo a modificar se encuentra en **/var/ossec/bin** y se llama ossec.conf. Los cambios se hacen después el campo de inicio de configuración del ossec. En este caso el tipo de formato es como la estructura de un "XML". Lo que agregamos es para la propiedad o etiqueta <client> y dentro de ella el campo <server-ip> con el valor del IP del servidor de OSSIM en este caso 192.168.0.59. Ver **Figura No 129**.

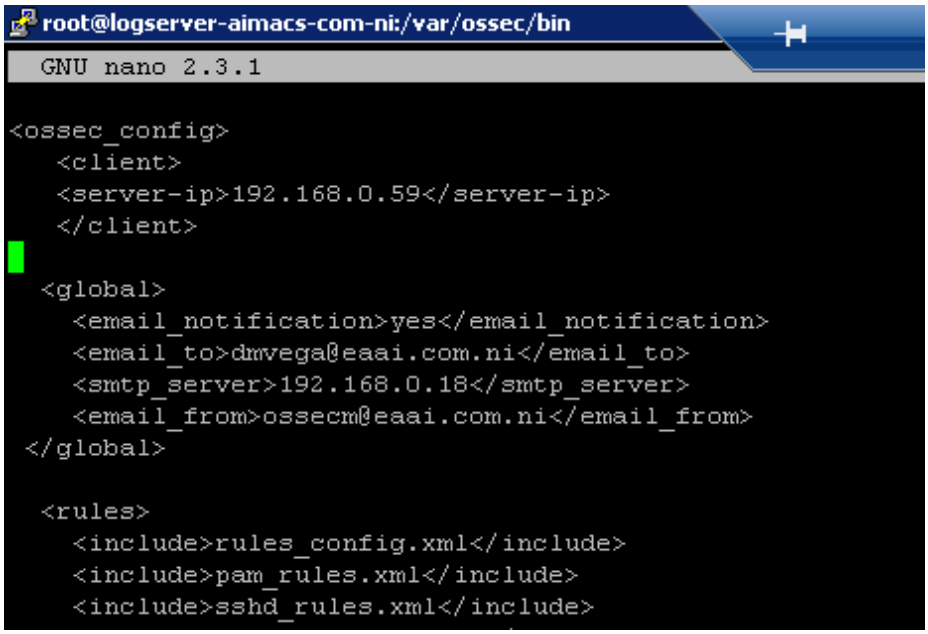


Figura No 129. Configuración de IP de OSSIM. (Captura de pantalla de equipo personal)

En la **Figura No 130** se observa que el agente está completamente configurado pero lo que hace falta es relacionar el agente con la clave cifrada del OSSIM que copiamos en el archivo de texto. Para eso en el directorio bin del agente ejecutamos el archivo "./manage_agent".

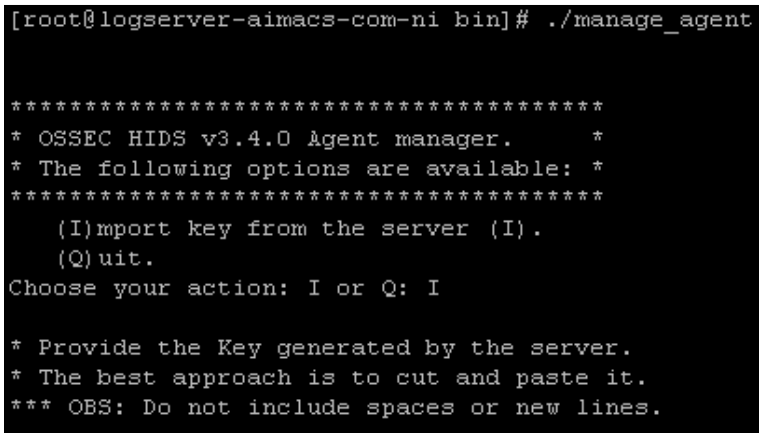
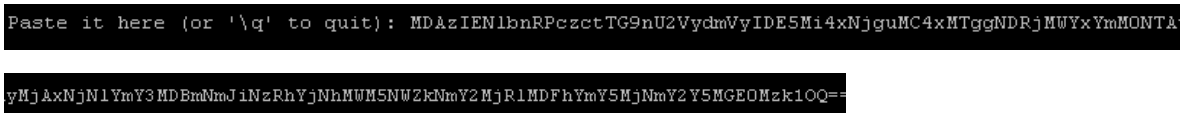


Figura No 130. Obtener Clave de Autenticación del Agente OSSEC (Captura de pantalla de equipo personal)

Para poder pegar la clave que relaciona con el OSSIM hay que escribir I, al inmediato nos dice que debemos proveer la clave generada por el servidor. Por tanto donde "Paste it here" (en español pegue aquí) pegamos la clave que tenemos en el bloc de notas.



Al inmediato cuando pegamos la clave el agente interpreta el texto cifrado de la misma forma con que la grabamos en el servidor de OSSIM. Lo único que queda es escribir "y" para confirmar que deseamos agregar la relación con el servidor. Tal como se muestra en la **Figura No 131.**

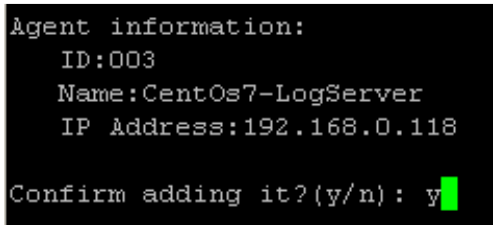


Figura No 131. Finalización configuración agente de OSSEC (Captura de pantalla de equipo personal)

Con lo anterior ha concluido la configuración del agente en el servidor de LOG. Ahora entramos a la administración web de OSSIM y localizamos el agente que creamos vía consola y que relacionamos vía comando en el servidor remoto de LOG.

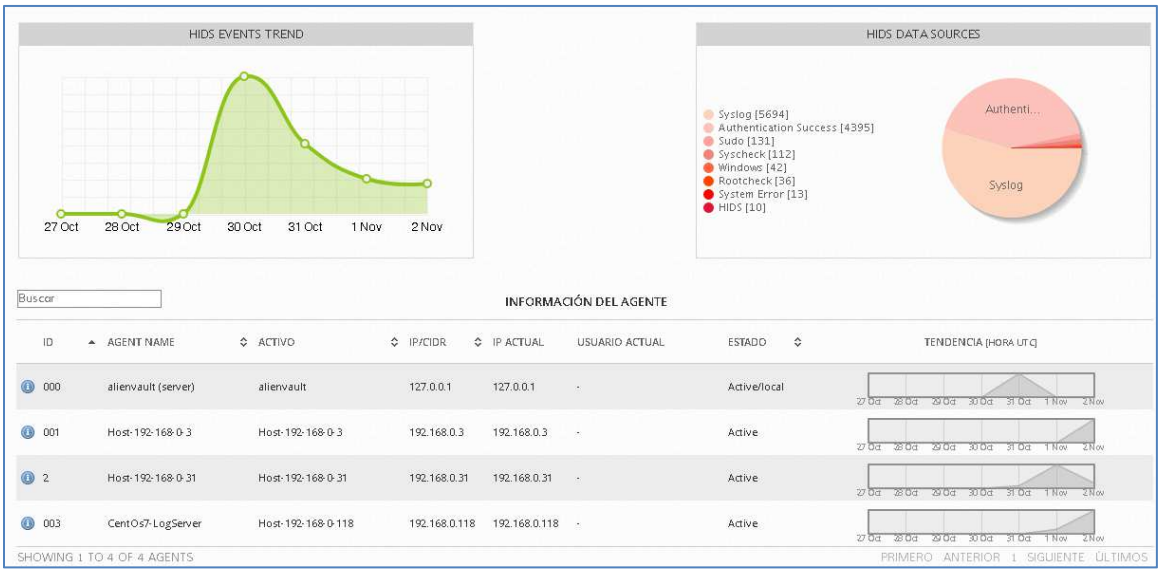


Figura No 132. Agente OSSEC Conectado (Captura de pantalla de equipo personal)

Finalmente hemos concluido la configuración de los agentes y podemos ver en detalle todas las opciones en menú "ENTORNO", sub-menú "AGENTES" y opción "AGENTE DE CONTROL". En esa ruta de menú encontramos la administración de todos los agentes instalados en OSSIM (Captura de pantalla de equipo personal).

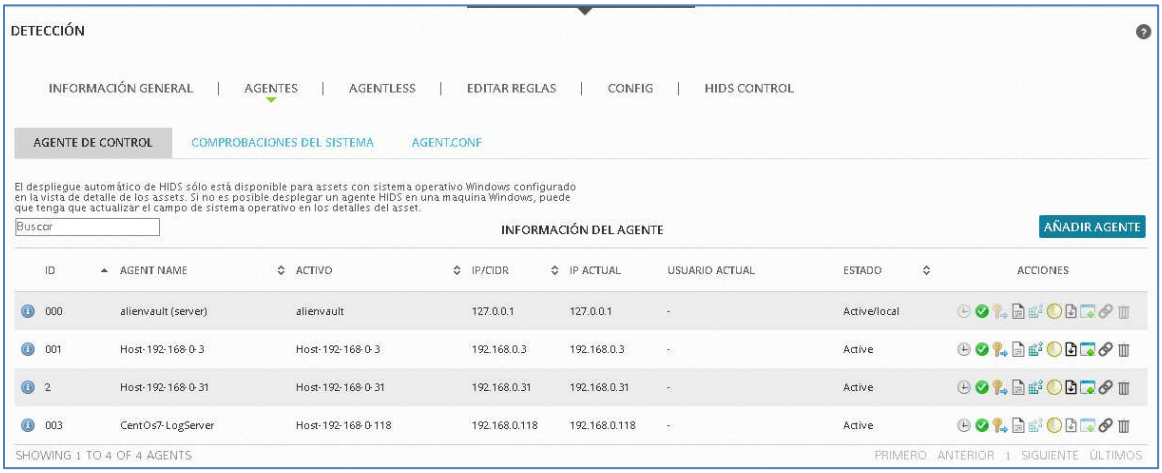


Figura No 133. Administración del agente OSSEC (Captura de pantalla de equipo personal)**.**

8.6. CONFIGURACIÓN DE REGLAS Y ALERTAS

La revisión del monitoreo de las alertas están basadas en las reglas que por defecto el SIEM activa; y otras que el OSSIM incorpora y podemos activar. A demás podemos crear nuestras propias reglas de acuerdo a los intereses que poseemos. A continuación se muestra la ruta en el web de las alertas. En el menú "ENTORNO" seleccionar sub-menú "DETECCION". Luego ir a la opción "CONFIG". En esa opción la **Figura No 134** muestra las reglas activas y las que pueden ser habilitadas por nosotros en OSSIM.

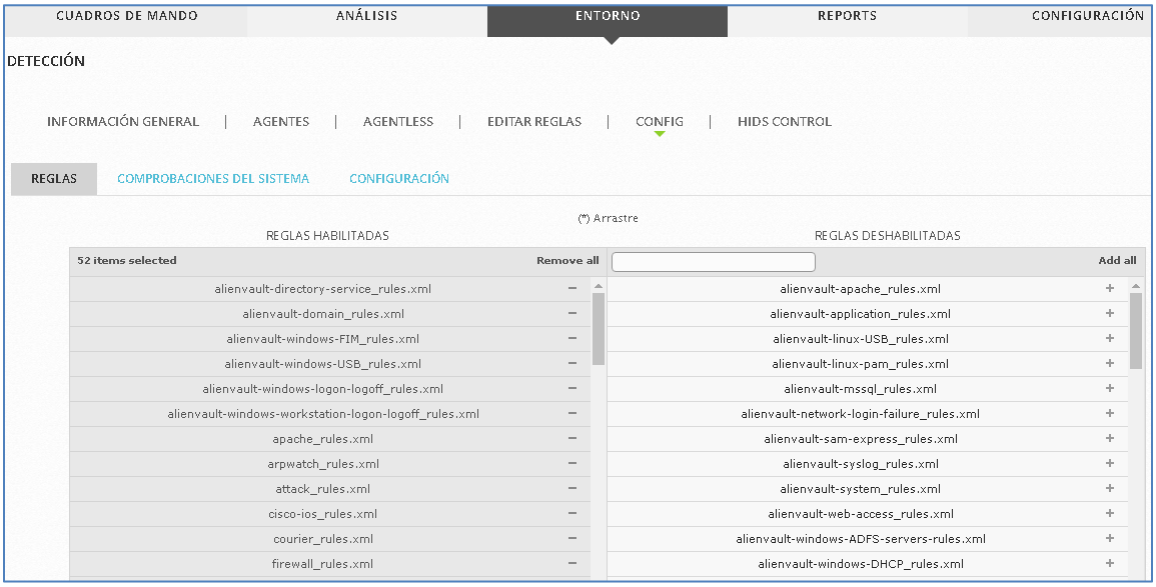


Figura No 134. Reglas de OSSIM (Captura de pantalla de equipo personal)

Al lado izquierdo están las reglas habilitadas y al lado derecho las no habilitadas. A continuación en la **Figura No 135** y **Figura No 136** mostraremos otras reglas.

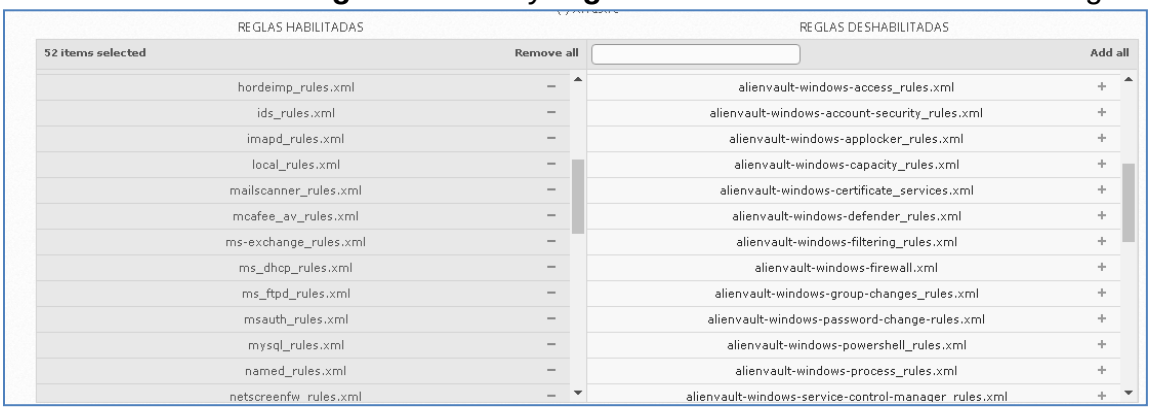


Figura No 135. Otras reglas 1 (Captura de pantalla de equipo personal)

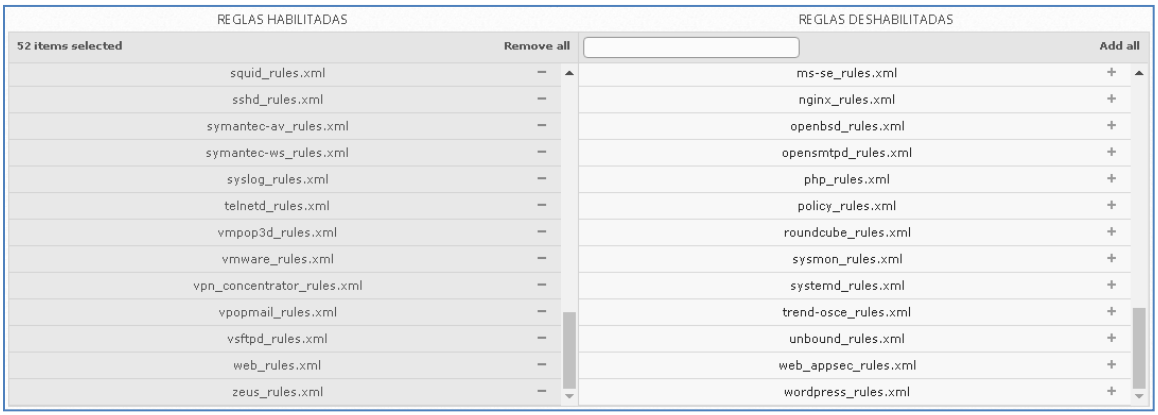


Figura No 136. Otras reglas 2 (Captura de pantalla de equipo personal)

En nuestro caso arrastraremos de izquierda a derecha las reglas que se enumeraran a continuación:

- alienvault-linux-pam_rules.xml
- alienvault-aplication_rules.xml
- alienvault-web-access_rules.xml
- aienvault-mssql_rules.xml
- alienvault-linux-USB.xml
- alienvault-network-login-failure_rules.xml
- alienvault-syslog_rules.xml
- alienvault-system_rules.xml
- alienvault-windows-account-security_rules.xml
- alienvault-windows-firewall.xml
- alienvault-windows-password-change-rules.xml
- alienvault-windows-powershell_rules.xml
- alienvault-windows-process_rules.xml
- alienvault-windows-shutdown_rules.xml
- alienvault-windows-access_rules.xml
- firewalld_rules.xml
- opensmtpd_rules.xml
- nginx_rules.xml

Para habilitar las reglas debemos simplemente arrastrarlas de izquierda a derecha o simplemente en las reglas deshabilitadas hacemos clic en el "+".

A continuación la imagen de las reglas ya habilitadas.

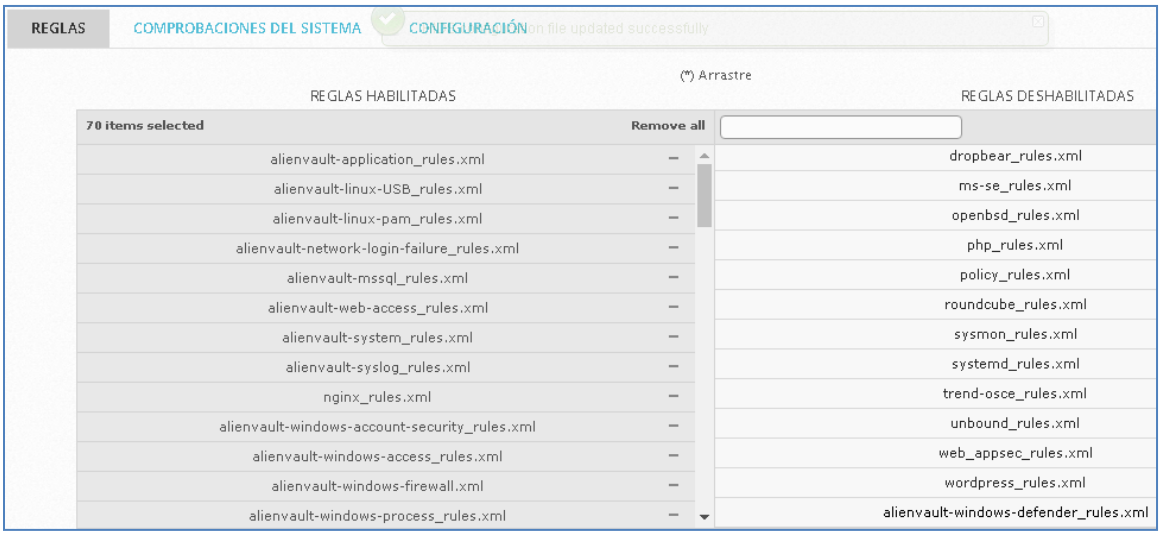


Figura No 137. Reglas nuevas habilitadas (Captura de pantalla de equipo personal)

En la **Figura No 137** se muestran que las reglas habilitadas ya no son 52, se han sumado 18 para un total de 70 reglas. Lo único que ahora queda por hacer es reiniciar los agentes instalados para que las reglas se apliquen en todos y el SIEM empiece a procesar este nuevo conjunto de reglas para la correlación y las alertas. En la **Figura No 138** nos ubicamos en menú "ENTORNO", sub-menú "DETECCION", buscamos "EDITAR REGLAS" y ahí se encuentra todo lo agregado.

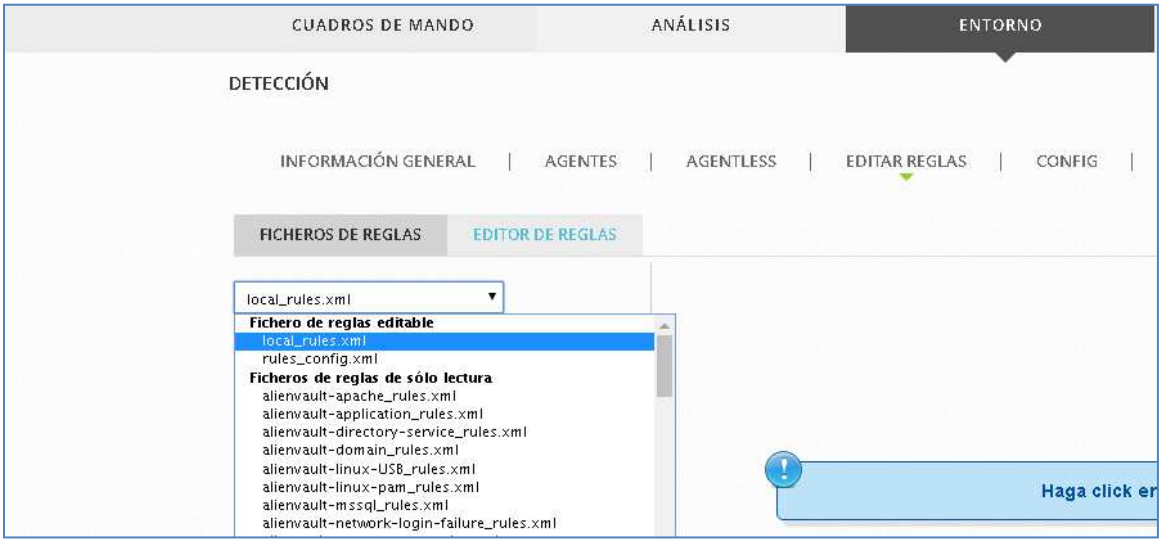


Figura No 138. Ubicación de Reglas para editar

Como se puede observar en la **Figura No 139** se han agregado todas las reglas y ahora podemos hacer uso de ellas. De hecho el motor de correlación y alertas lo está haciendo.

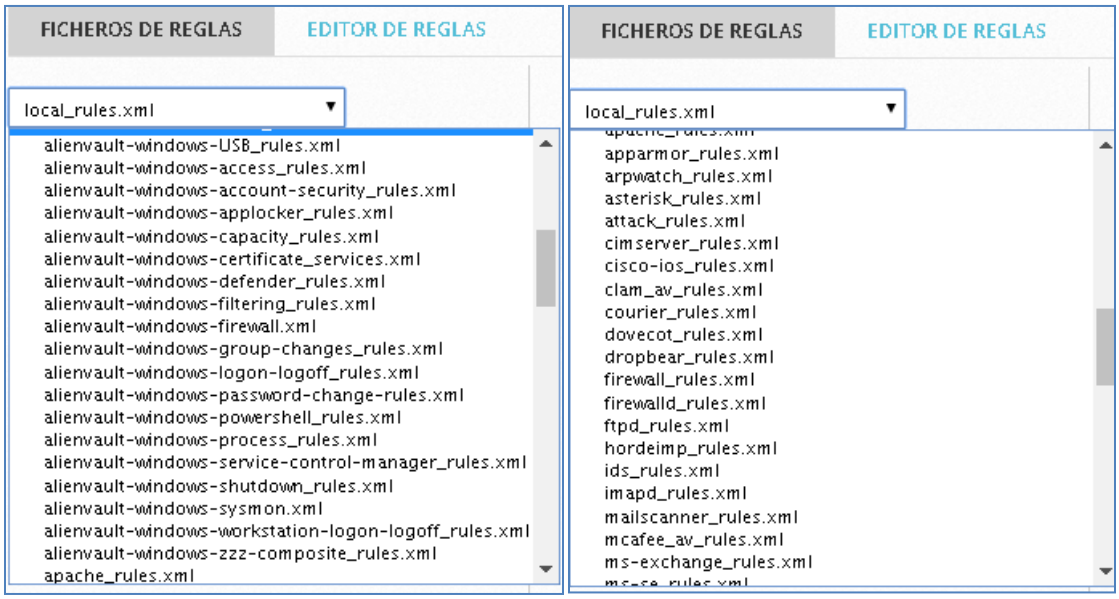


Figura No 139. Editor de Reglas (Captura de pantalla de equipo personal)

La **Figura No 140** muestra la regla seleccionada sshd_rules.xml. Para editarla hacemos clic en "EDITOR DE REGLAS" .

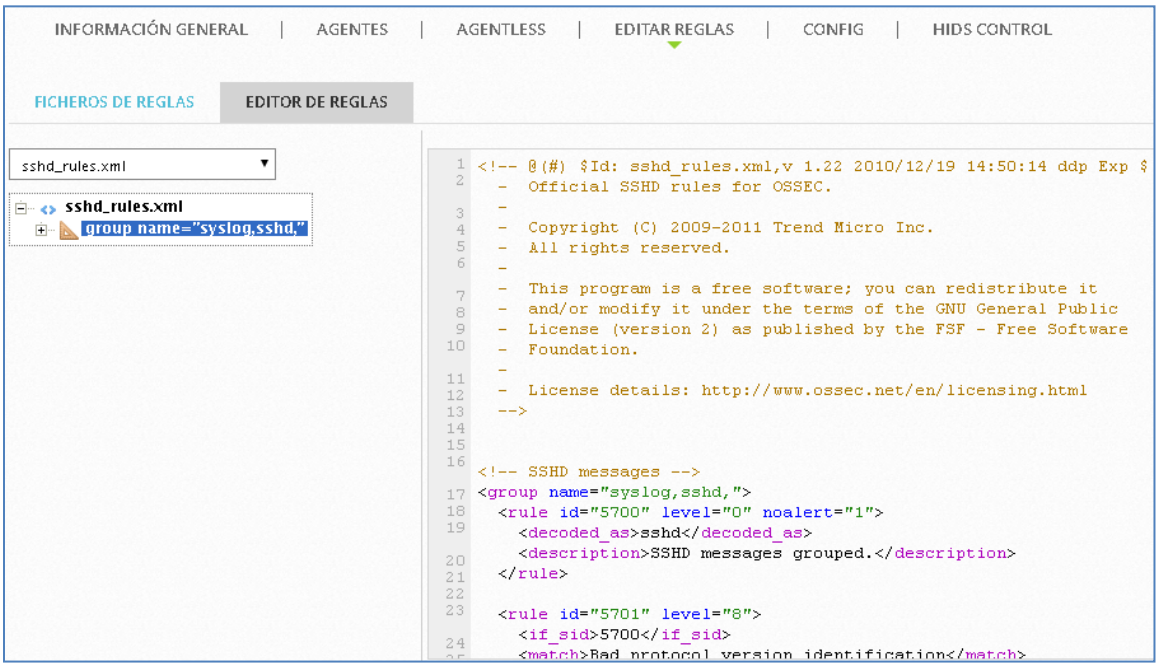


Figura No 140. Edición de Regla SSHD 1 (Captura de pantalla de equipo personal)

Como claramente nos muestra la **Figura No 140** el nombre del archivo de reglas al final su extensión es un XML. Por tato ya conocemos cual es la sintaxis del mismo. De tal forma que podríamos con buena experiencia modificar o crear

nuestras propias reglas. Las reglas del archivo XML están compuestas por un inicio y fin con la palabra clave "rule". Luego dentro de ella se declaran las variables o propiedades a utilizar.

Por ejemplo: La palabra "rule" como inicio de la regla acompañada con "id" y "level" como encabezado principal de la misma. "id" es el código del evento y "level" es el nivel de gravedad del mismo.

```
<rule id="5702" level="5">
```

Se muestra el campo "if_sid" que al igual que "rule" al inicio va entre "< >" y al final igual pero inicia con una "/"

```
<if_sid>5700</if_sid>
```

El campo "match" al igual que "regex" son utilizados para relacionar los factores de búsqueda de la regla. En este caso son cadenas de texto para ambos. Pero "regex" es también para expresiones regulares.

```
<match>^reverse mapping</match>
<regex>failed - POSSIBLE BREAK</regex>
```

El campo "description" es donde escribimos el mensaje del evento relacionado. Puede haber más de uno.

```
<description>Reverse lookup error (bad ISP or attack).</description>
```

```
</rule>
```

Con esta etiqueta "/rule" finalizamos la configuración de la regla.

Es importante señalar que para poder diseñar una reglas es necesario conocimiento amplio del protocolo que se está utilizando para la regla a crear. En este caso puede resultar útil utilizar software como **wireshark** para ver que pasa cada vez que establecemos una conexión con cualquier protocolo. Los elementos comunes los podemos asociar con una expresión regular en la creación de la regla.

A continuación en la **Figura No 141** mostramos contenidos parciales de la regla de **sshd**. En esa regla se puede observar que existen validaciones que alertan de comportamientos como tiempos de esperas agotados y hasta intentos de escaneos al puerto TCP 22. (SSH)

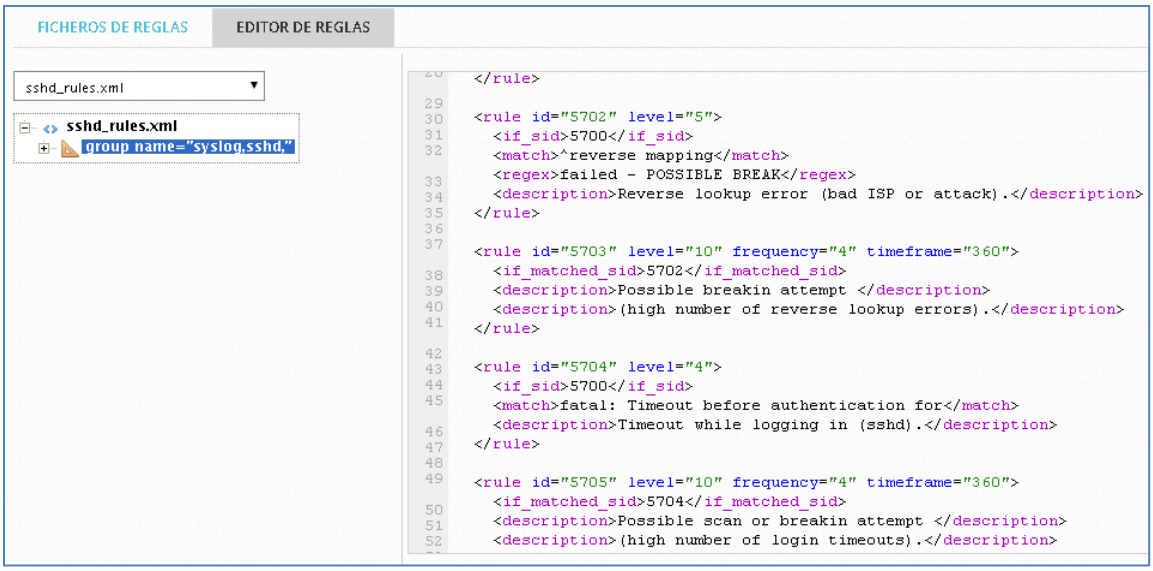


Figura No 141. Edición de regla ssd 2 (Captura de pantalla de equipo personal)

De igual forma la **Figura No 142** muestra el código de la regla para opensmtpd_rules.xml. Podemos observar que como agrupa a varias reglas lleva al inicio la palabra clave "group" acompañado de la palabra "name" para indicar el nombre del grupo de reglas. En este caso indica que funciona para un **syslog server** de un servidor de correos con "**smtpd**" como servicio.

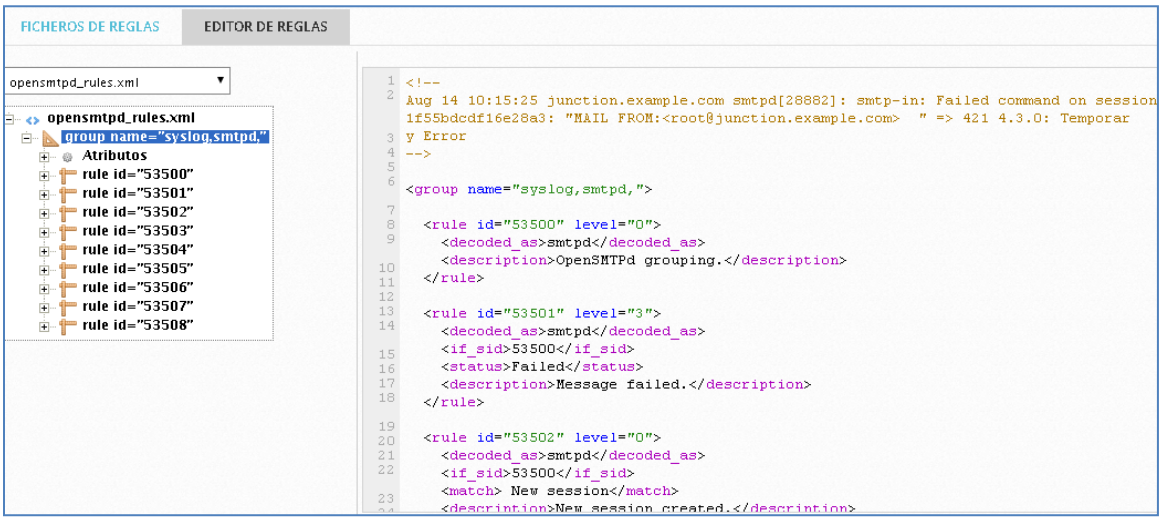


Figura No 142. Edición de regla smtpd 1 (Captura de pantalla de equipo personal)

En la **Figura No 143** se observa el final de la regla "**smtpd**"; nótese que al igual que al inicio de la regla en la **Figura No 142** se utiliza la palabra "group". En este caso se utiliza para cierre respetando la sintaxis del XML.

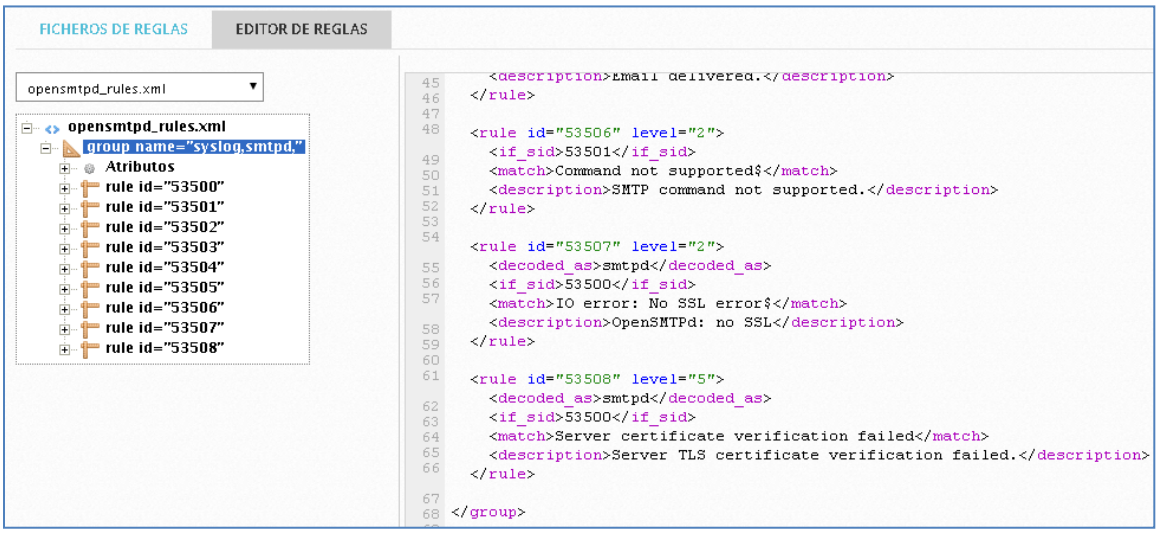


Figura No 143. Edición de regla smtpd 2 (Captura de pantalla de equipo personal)

8.7. REVISIÓN Y MONITOREO DE EVENTOS

Para el monitoreo y la revisión de eventos generados por las distintas fuentes de datos del SIEM podemos hacerlos de dos formas. La primera es ir a los "CUADROS DE MANDO" y seleccionar "INFORMACION GENERAL". Estando ahí podemos ver varias opciones como: "EXECUTIVE", "TICKETS", "SECURITY, TAXONOMY" y "VULNERABILITIES". En cualquiera de esos sub-menús encontramos información inmediata de los aspectos más relevantes que están ocurriendo en la red. En este caso la opción "EXECUTIVE" mostrada en la **Figura No 144** muestra la siguiente información:

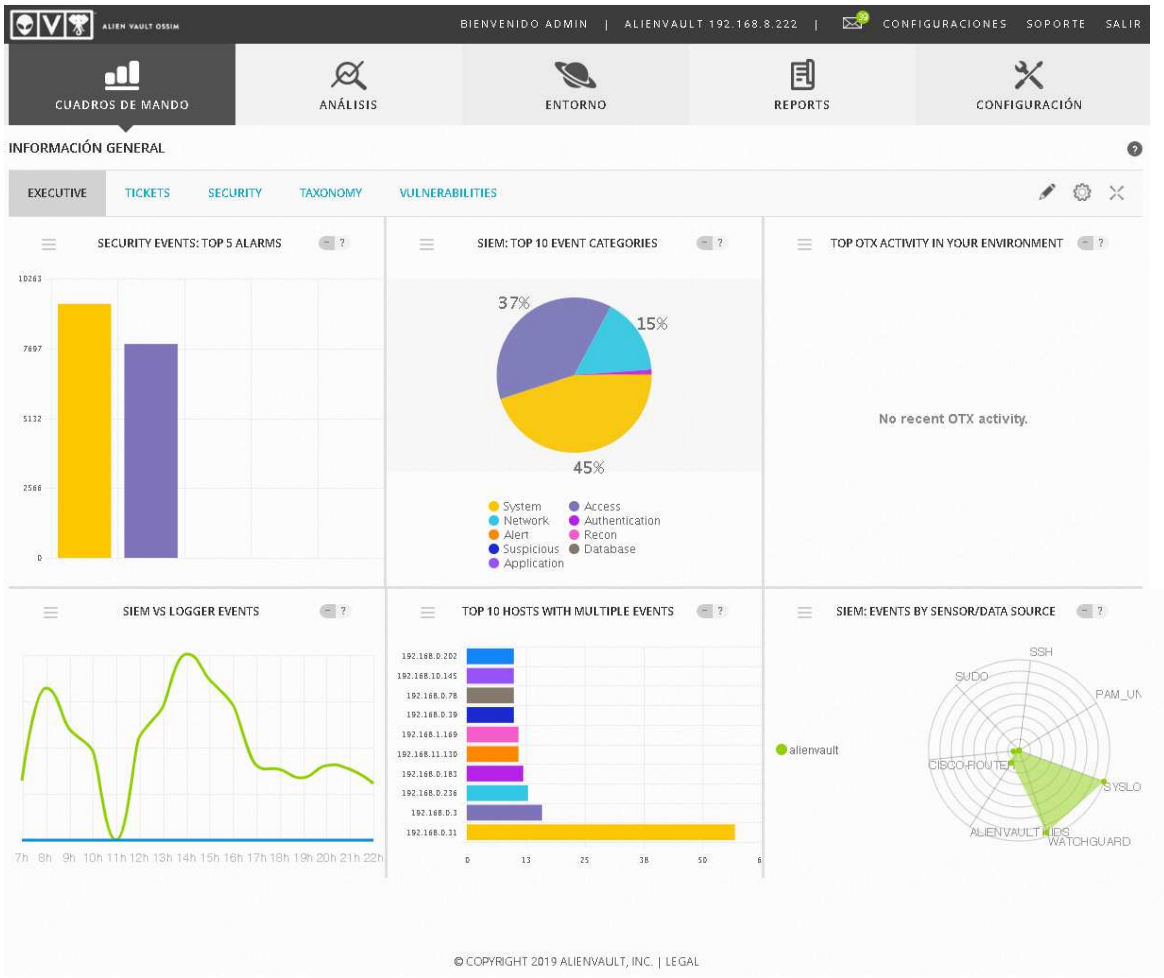


Figura No 144. Cuadro de Mando Ejecutivo (Captura de pantalla de equipo personal)

En la **Figura No 144** se pueden observar 6 cuadros que de izquierda a derecha y de arriba abajo muestran información general de: Las alarmas, eventos por categorías, actividad de OTX, gráfico de eventos en el tiempo, los 10 host con más eventos y el diagrama de las fuentes de datos que más eventos generan.

Si nos posicionamos sobre el cuadro de mando de "SECURITY EVENTES: TOP 5 ALARMS" (en español Eventos de Seguridad: Las 5 alarmas principales) mostrado en la **Figura No 145** y nos colocarnos en la primera barra de la izquierda muestra el número de alarmas de ese evento.

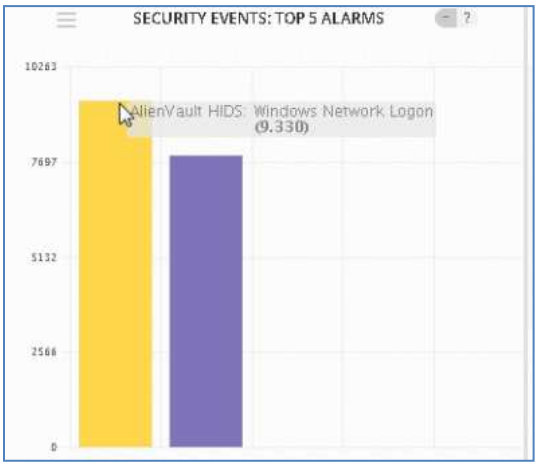


Figura No 145. Eventos de Seguridad, 5 más altos (Captura de pantalla de equipo personal)**.**

Si hacemos clic en una alarma nos mostrará la información detallada de todos los eventos que la generaron. Como se observa en la **Figura No 146** el SIEM se dirigió al menú "ANALISIS" y luego al sub-menú "ALARMAS". En el cual por defecto abrió en la "VISTA LISTA". En general existen opciones de búsquedas que podemos aplicar. La alarma se muestra después de las fechas.

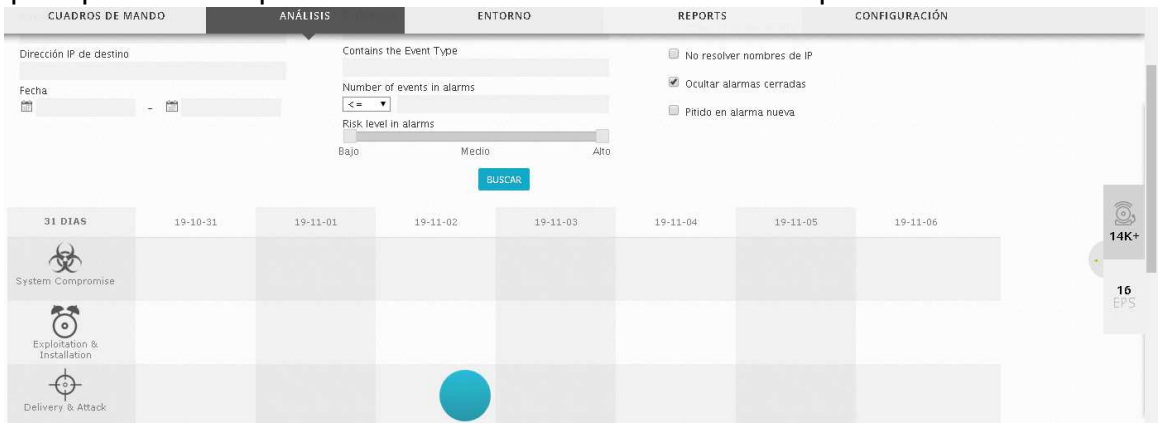


Figura No 146. Alarma de ataque deliberado (Captura de pantalla de equipo personal)

Si hacemos clic sobre el evento que está en el **círculo** del día 2 de noviembre en la **Figura No 146** se mostrará el detalle de los eventos que dieron origen a ese ataque. Tal como se observa en la **Figura No 147**.

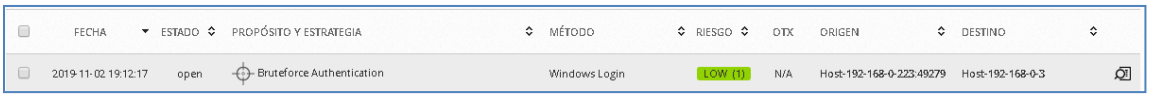


Figura No 147. Información de evento de alarma generada (Captura de pantalla de equipo personal)

En la **Figura No 147** pudimos observar en el evento producido el origen y destino del ataque. A demás al hacer clic sobre el icono que tiene una hoja con una lupa a un lado nos cargará la información mostrada en la **Figura No 148**.

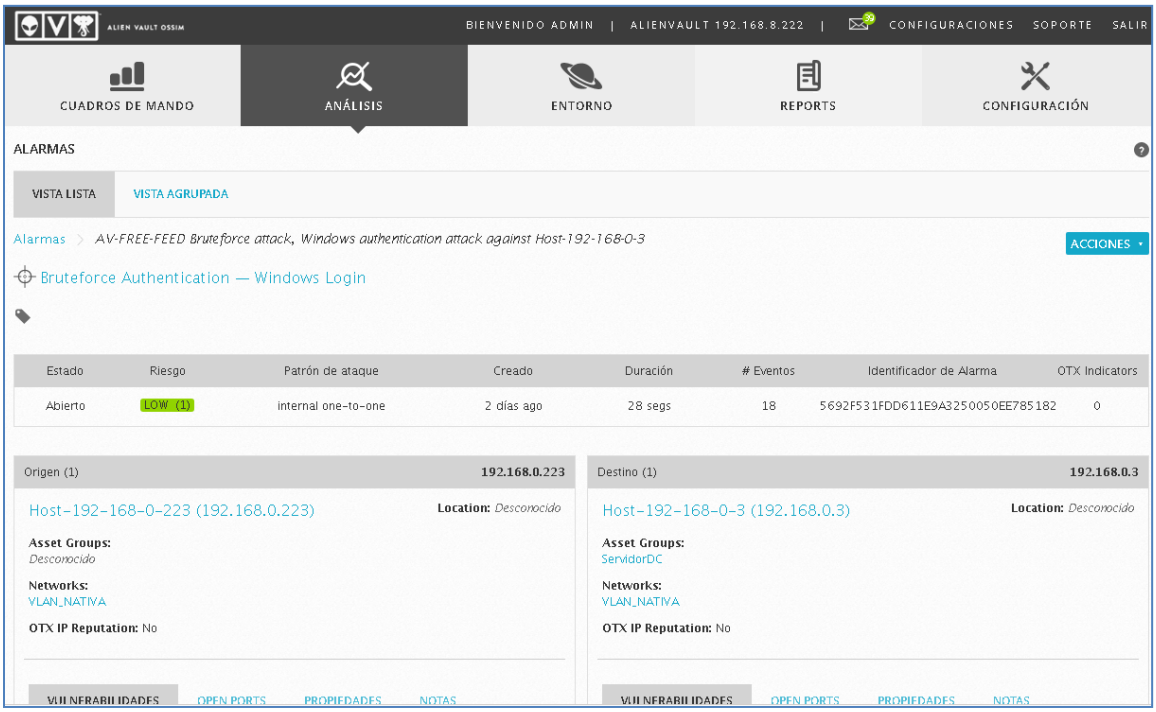
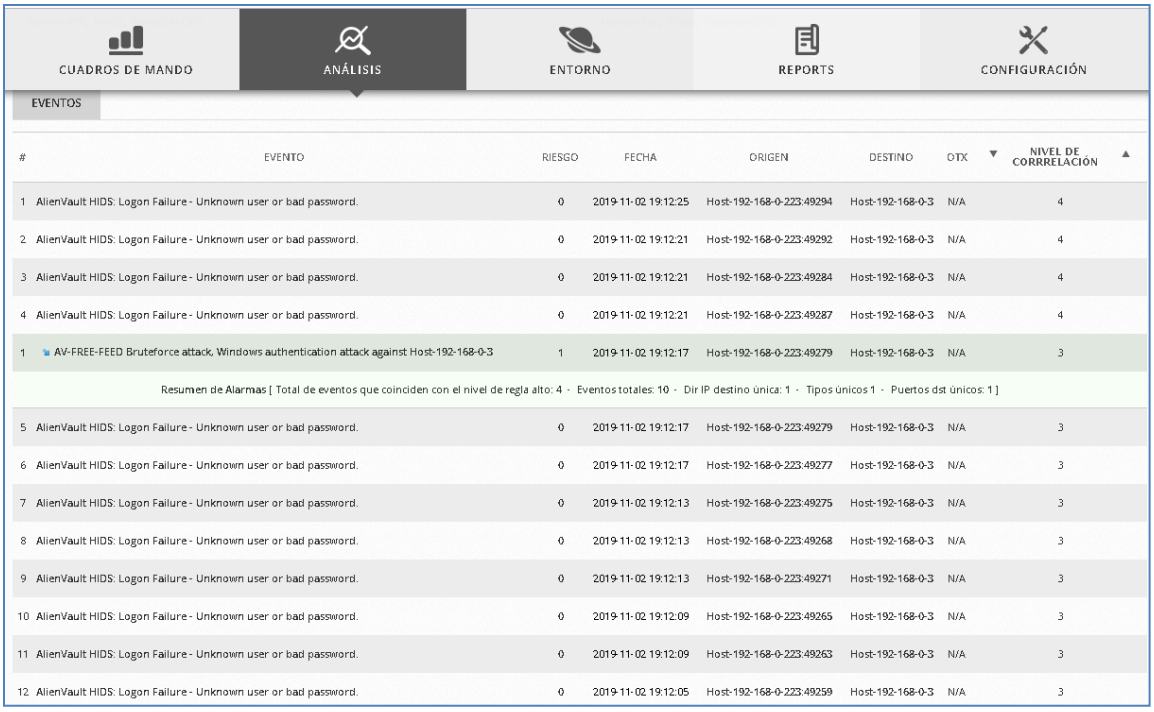


Figura No 148. Detalle de alarma en evento Bruteforce Authentication (Captura de pantalla de equipo personal)

Como se observa en la **Figura No 148** la alarma la generó el HIDS que está instalado en el equipo con IP 192.168.0.3 y el ataque fue una autenticación por ataque de fuerza bruta. Estos provinieron del equipo 192.168.0.223. Más debajo de la descripción de los IPs se localizan otras opciones como ver vulnerabilidades, puertos, servicios y severidad.

Los eventos que desataron la alarma de la **Figura No 148** son los siguientes:



#	EVENTO	RIESGO	FECHA	ORIGEN	DESTINO	OTX	NIVEL DE CORRELACIÓN
1	AlienVault HIDS: Logon Failure - Unknown user or bad password.	0	2019-11-02 19:12:25	Host-192-168-0-223:49294	Host-192-168-0-3	N/A	4
2	AlienVault HIDS: Logon Failure - Unknown user or bad password.	0	2019-11-02 19:12:21	Host-192-168-0-223:49292	Host-192-168-0-3	N/A	4
3	AlienVault HIDS: Logon Failure - Unknown user or bad password.	0	2019-11-02 19:12:21	Host-192-168-0-223:49284	Host-192-168-0-3	N/A	4
4	AlienVault HIDS: Logon Failure - Unknown user or bad password.	0	2019-11-02 19:12:21	Host-192-168-0-223:49287	Host-192-168-0-3	N/A	4
1	AV-FREE-FEED Bruteforce attack, Windows authentication attack against Host-192-168-0-3	1	2019-11-02 19:12:17	Host-192-168-0-223:49279	Host-192-168-0-3	N/A	3
	Resumen de Alarmas [Total de eventos que coinciden con el nivel de regla alto: 4 · Eventos totales: 10 · Dir IP destino única: 1 · Tipos únicos 1 · Puertos dst únicos: 1]						
5	AlienVault HIDS: Logon Failure - Unknown user or bad password.	0	2019-11-02 19:12:17	Host-192-168-0-223:49279	Host-192-168-0-3	N/A	3
6	AlienVault HIDS: Logon Failure - Unknown user or bad password.	0	2019-11-02 19:12:17	Host-192-168-0-223:49277	Host-192-168-0-3	N/A	3
7	AlienVault HIDS: Logon Failure - Unknown user or bad password.	0	2019-11-02 19:12:13	Host-192-168-0-223:49275	Host-192-168-0-3	N/A	3
8	AlienVault HIDS: Logon Failure - Unknown user or bad password.	0	2019-11-02 19:12:13	Host-192-168-0-223:49268	Host-192-168-0-3	N/A	3
9	AlienVault HIDS: Logon Failure - Unknown user or bad password.	0	2019-11-02 19:12:13	Host-192-168-0-223:49271	Host-192-168-0-3	N/A	3
10	AlienVault HIDS: Logon Failure - Unknown user or bad password.	0	2019-11-02 19:12:09	Host-192-168-0-223:49265	Host-192-168-0-3	N/A	3
11	AlienVault HIDS: Logon Failure - Unknown user or bad password.	0	2019-11-02 19:12:09	Host-192-168-0-223:49263	Host-192-168-0-3	N/A	3
12	AlienVault HIDS: Logon Failure - Unknown user or bad password.	0	2019-11-02 19:12:05	Host-192-168-0-223:49259	Host-192-168-0-3	N/A	3

Figura No 149. Todos los eventos que generaron la alarma de Falla de inicio (Captura de pantalla de equipo personal)

Todos los eventos generados en la Figura No 149 muestran a la izquierda el tipo de actividad ejercida y la fuente de la misma alerta. En este caso la fuente es el "HIDS" y la falla es "Logon Failure- Unknown user or bad password" (en español Falla de inicio de sesión – Usuario desconocido o clave errónea). Brinda a demás dirección IP del atacante y el destino. Un dato importante es el nivel de correlación del evento.

Si hacemos clic sobre cualquier evento generado en la **Figura No 149** nos dará el detalle más completo de lo ocurrido. Tal como se observa en la **Figura No 150** los datos ya normalizados por el SIEM donde nos dice los campos: "NOMBRE DE USUARIO", "USERDATA1" AL "USERDATA9". Toda esa información es obtenida del LOG original recibido en formato RAW.

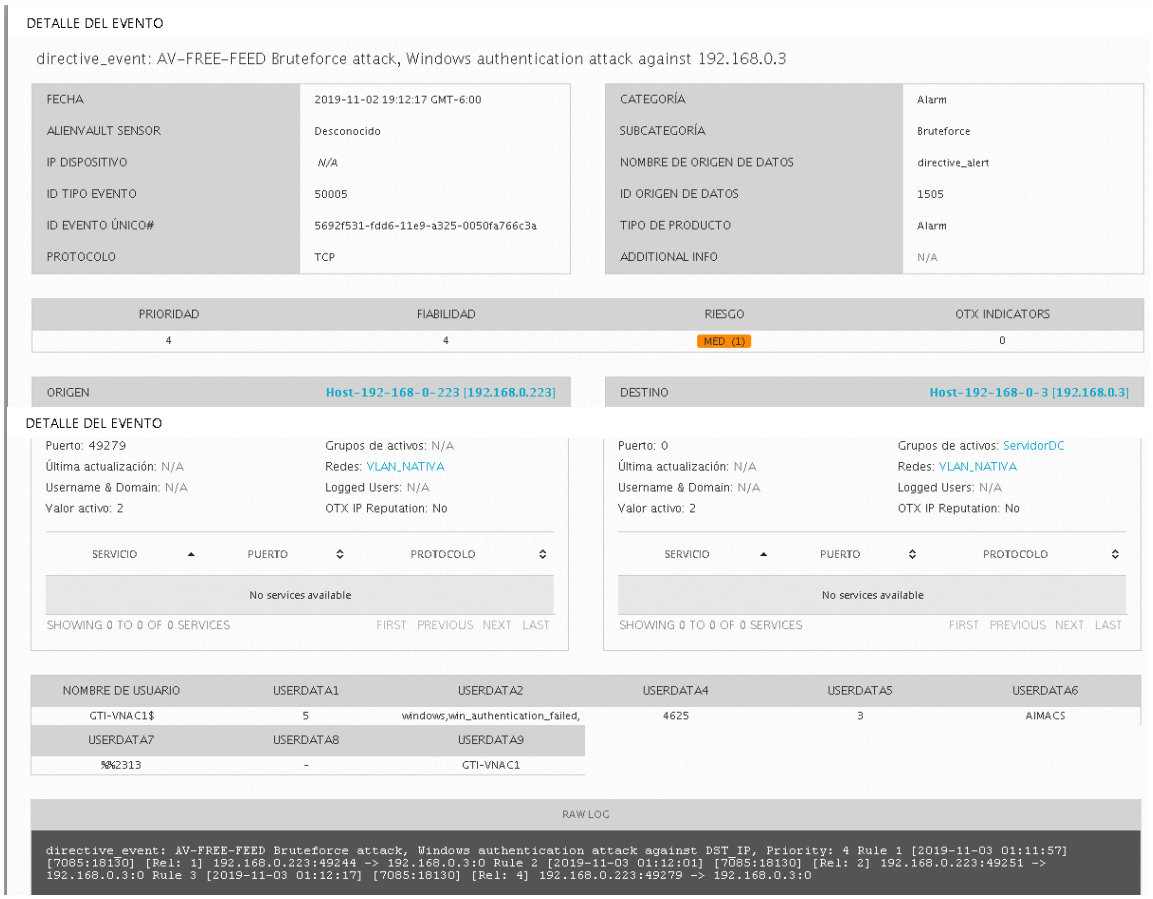


Figura No 150. Detalle completo del evento de ataque (Captura de pantalla de equipo personal)

El monitoreo de eventos también puede darse directamente cuando vamos al menú "ANALISYS" y seleccionamos sub-menú "EVENTOS SIEM". Nos muestra por defecto la lista de eventos de la última hora. En el criterio de búsqueda o filtro aparece "Last Hour". Como se observa en la **Figura No 151** hay un buen listado de eventos que podemos seleccionar para ver detalle de lo que nos pueda llamar la atención.

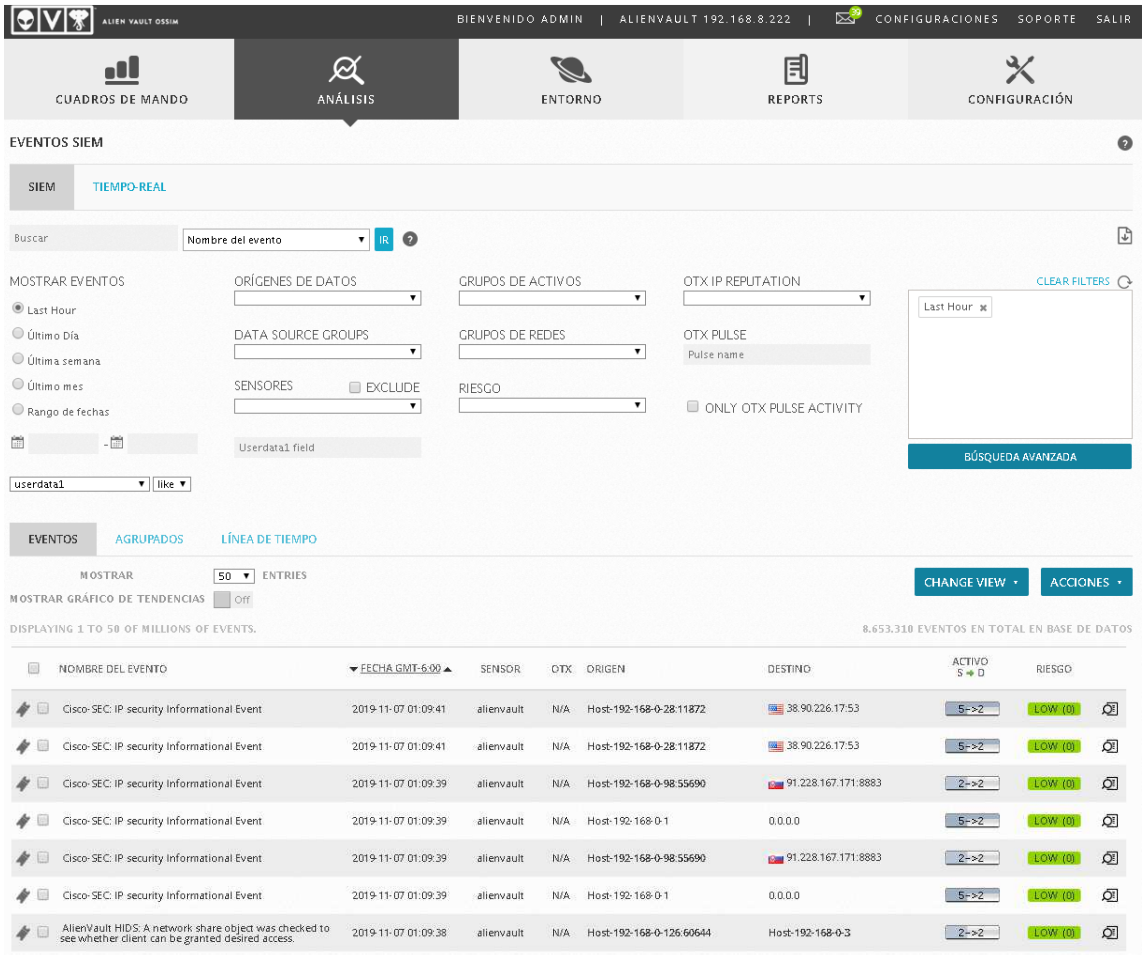


Figura No 151. Eventos SIEM (Captura de pantalla de equipo personal)

En el monitoreo los cuadros de mando nos permiten de inmediato ir y prestar atención de lo que está ocurriendo. En el sub-menú "INFORMACION GENERAL" seleccionamos la opción "TAXONOMY" (en español taxonomía), esta opción nos da como una radiografía general del más crítico que está ocurriendo. Tal como se muestra en la **Figura No 152**.

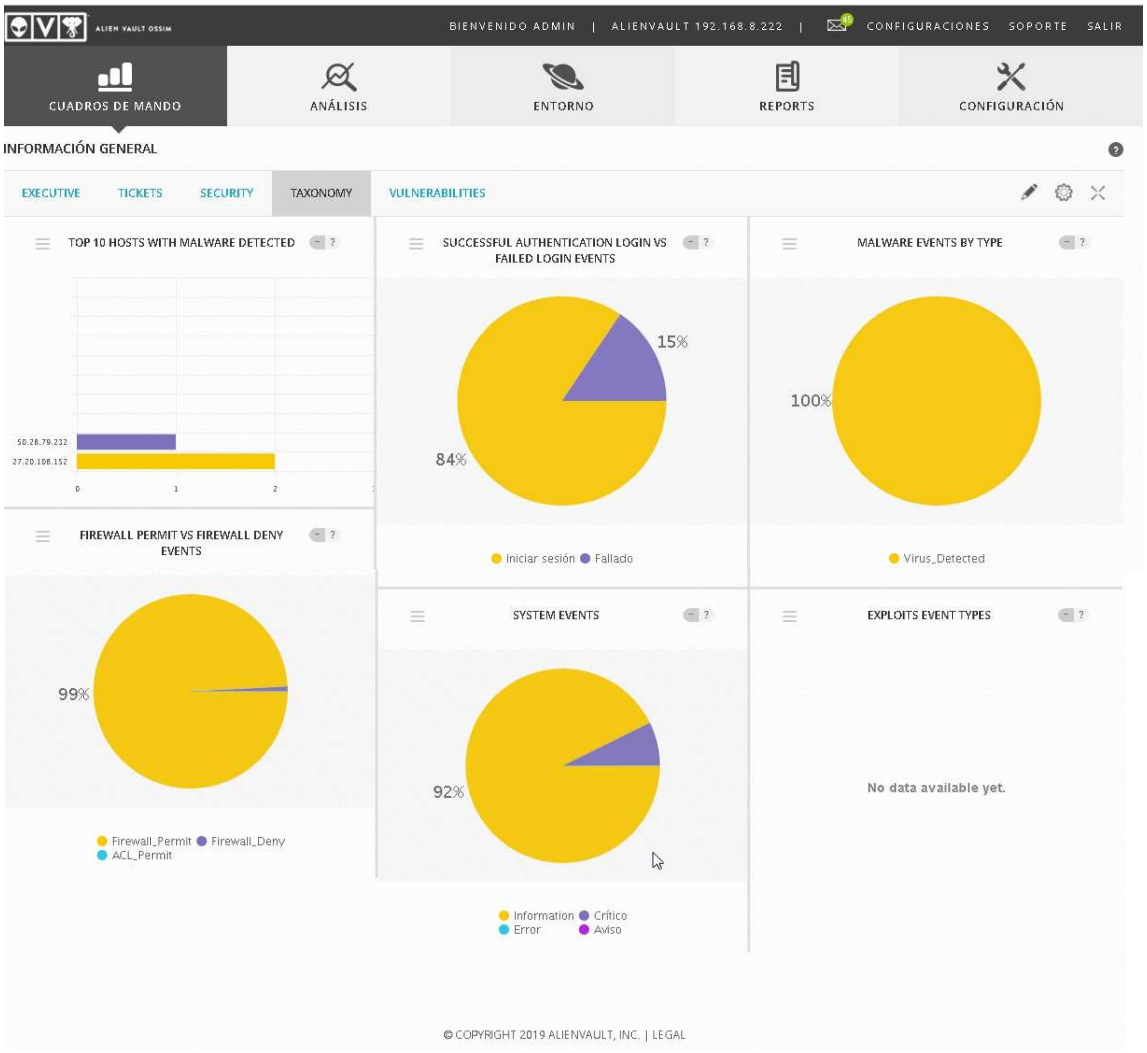


Figura No 152. Cuadro de Mando Taxonomía (Captura de pantalla de equipo personal)

En este caso lo más relevante es la detección de malware que se detecta en los 10 host con detección de malware (**TOP 10 HOSTS WITH MALWARE DETECTED**) y es la misma que se detecta en eventos malware por tipo (**MALWARE EVENTS BY TYPE**). Al hacer clic en el gráfico de **MALWARE EVENTS BY TYPE** (En español eventos malware por tipo) de la **Figura No 152** nos aparece la lista de eventos del momento tal y como se muestra en la **Figura No 153**.

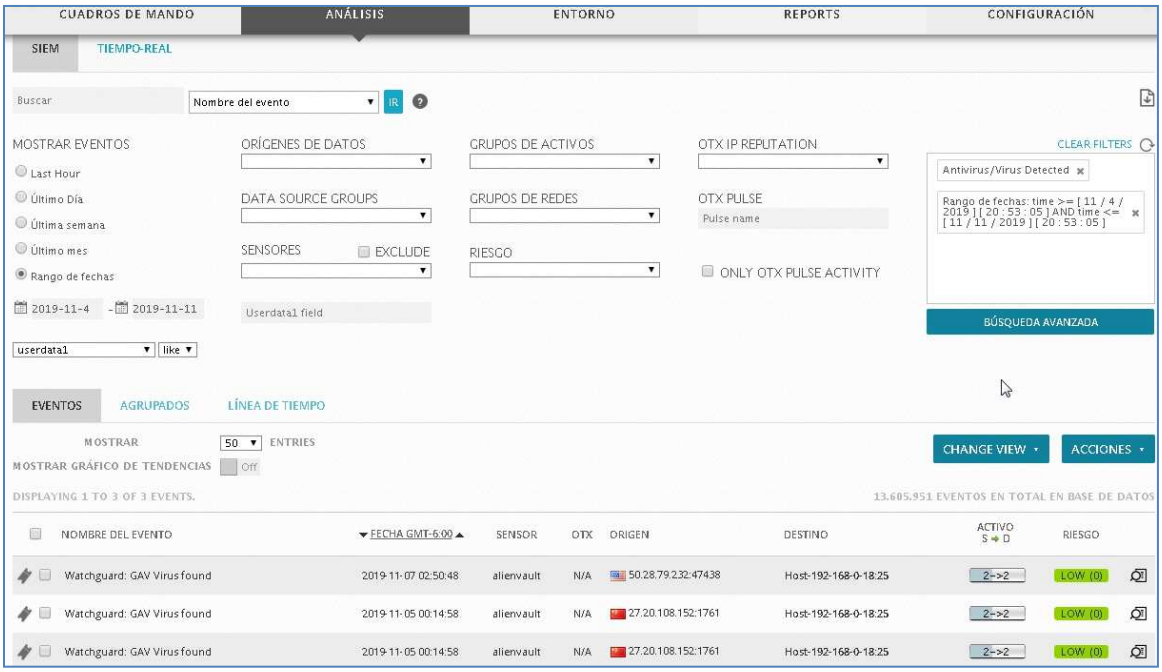


Figura No 153. Eventos de Virus generados por cuadro de mando taxonomía (Captura de pantalla de equipo personal)

Si seleccionamos cualquiera de los eventos y hacemos clic en el icono de la hoja con la lupa nos aparecerá en detalle lo ocurrido. En ese caso el primer evento nos muestra su origen y el puerto destino. En este caso fue por medio de correo. Tal como se observa en la **Figura No 154**.

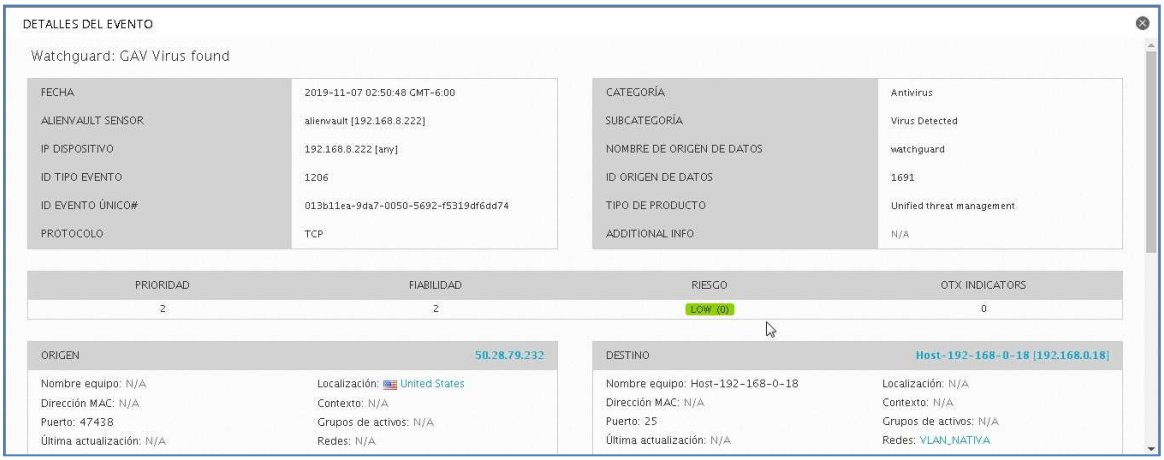


Figura No 154. Detalle de evento de virus 1 (Captura de pantalla de equipo personal)

Al seguir bajando en el detalle del evento, ver **Figura No 155**, podemos apreciar más detalles de lo ocurrido. Nos dice que el evento fue de origen externo, no solo por el hecho de la IP vista en la imagen anterior era pública sino por

decirnos en campo de geolocalización que provenía de U.S.A. en el detalle del archivo en bruto (RAW LOG) nos da la información de que el que envió el mensaje fue info@nitul.in y que el destino era el correo comercial@eaai.com.ni , a demás dice que el virus o malware era un "Trojan.Agent.DWSC" que venía camuflado en un archivo de Word con el nombre "02061179.doc".

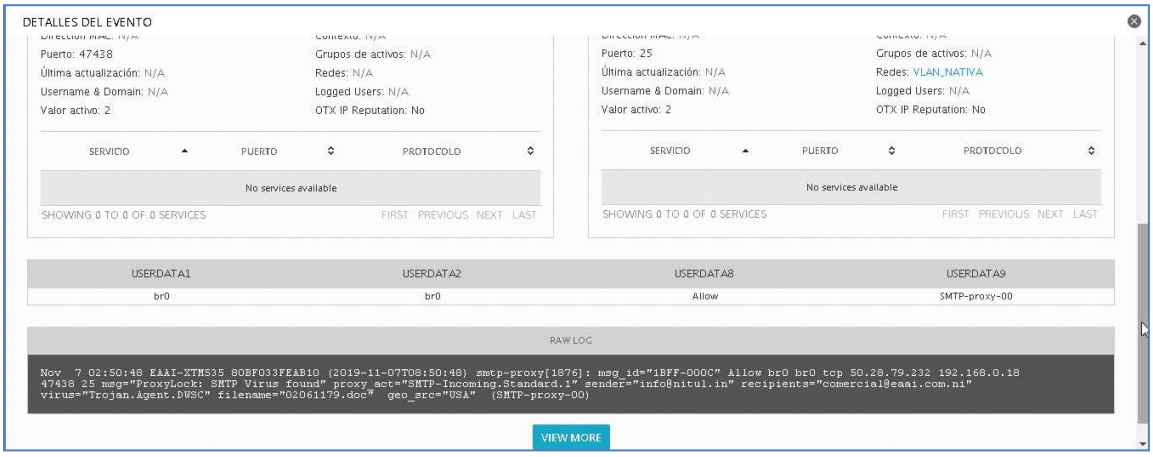


Figura No 155. Detalle de evento de virus 2 (Captura de pantalla de equipo personal)

9. PRUEBAS Y AJUSTES DE SIEM

9.1. PRUEBAS DE SIEM

Para llevar a cabo pruebas del SIEM se realizaron ingresos fallidos a propósito y en un ataque de fuerza bruta ha quedado evidenciado en las alarmas descritas. Durante el proceso de pruebas del SIEM se observa que hemos realizado en menú, "ANALISIS", sub-menú "EVENTOS SIEM", una búsqueda por medio de filtros. En este caso el IP 192.168.0.62 como origen y donde la variable time (tiempo) sea mayor o igual a 29 de octubre de 2019. Ver **Figura No 156**.

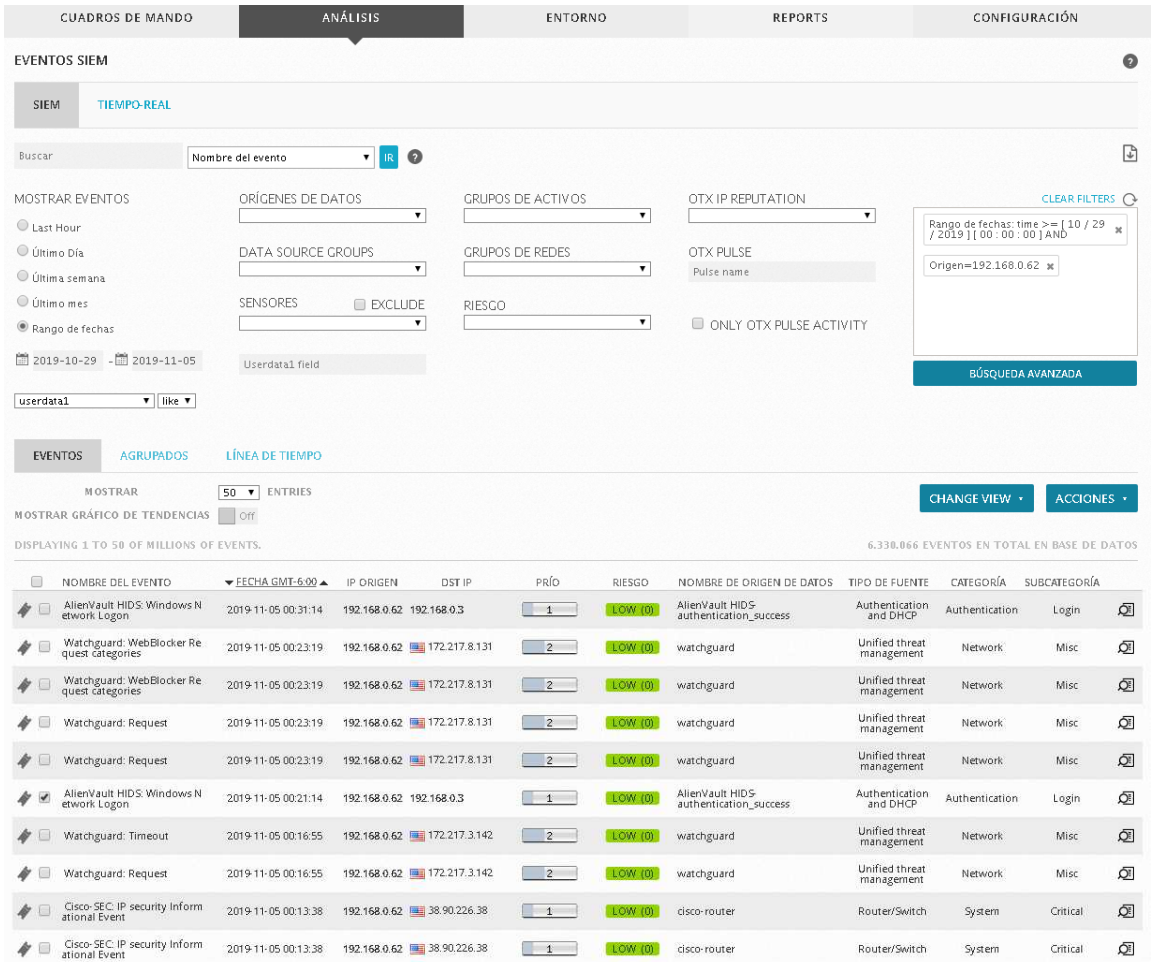


Figura No 156. Búsqueda de eventos SIEM (Captura de pantalla de equipo personal)

Para las pruebas se ha elegido una autenticación correcta para observar en detalle como el SIEM brinda información. Se observa en la **Figura No 158** que la categoría ha sido un inicio de sesión (Login), hay detalles de "ID TIPO EVENTO" que es el 700003. Del equipo destino se obtiene la dirección física de

la tarjeta de red (MAC). En el campo NOMBRE DE USUARIO nos devuelve "**dcorea**" y desde USERDATA1 AL USERDATA9 muestra información relevante como: Sistema operativo (Windows), tipo de servicio (Windows Network Logon) y dominio (AIMACS.COM.NI). Todo esto producto de la normalización efectuada al archivo RAW del LOG.

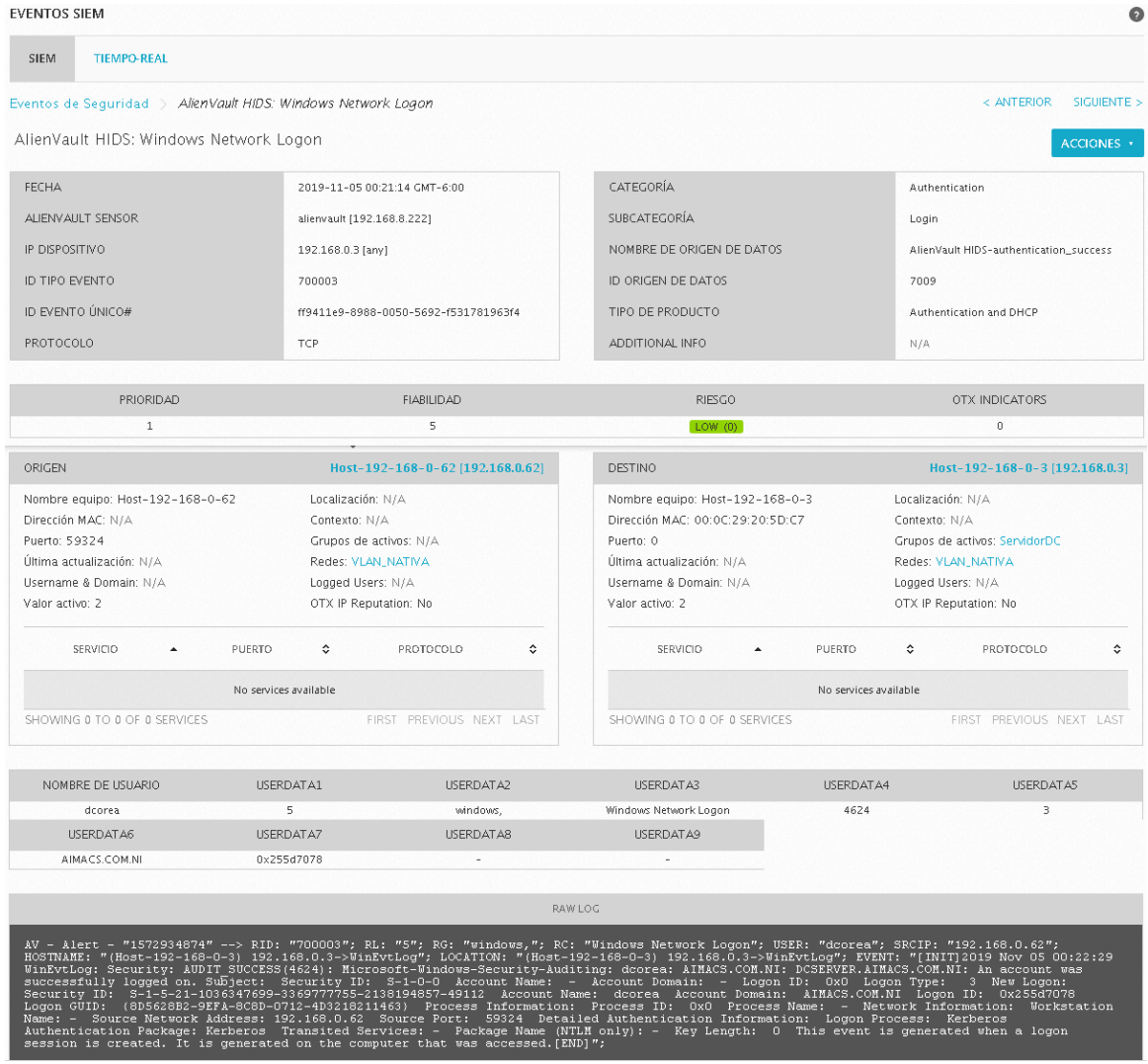


Figura No 157. Evento de Inicio de sesión en un SIEM (Captura de pantalla de equipo personal)

El evento anterior en el SIEM es fácil de entender y de encontrar. En cambio si vamos a los LOG del servidor la cosa es más compleja. Por ejemplo un inicio de sesión. Tal como se muestra en la **Figura No 158**.

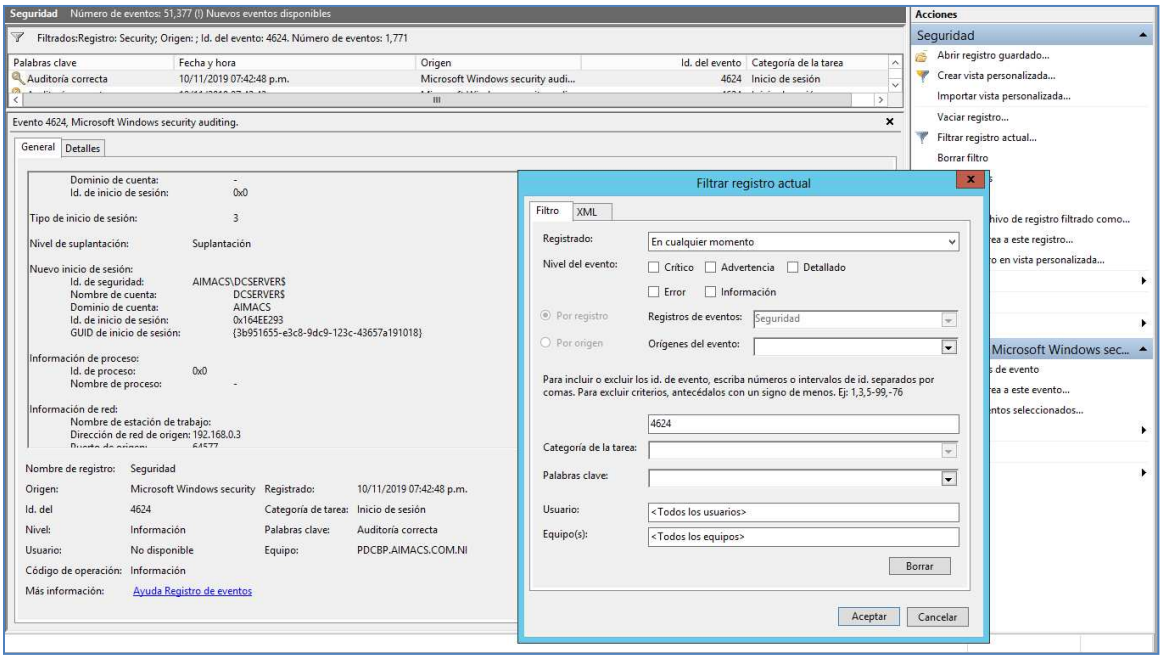


Figura No 158. Evento de inicio de sesión en Windows Server (Captura de pantalla de equipo personal)

En esta imagen mostrada en la **Figura No 158** se describen todos los eventos del servidor Windows 2016. En este caso para buscar el evento hay que establecer filtros y tener conocimientos de los id de eventos y otros datos del sistema operativo para que la búsqueda sea efectiva. En este caso se seleccionó el registro de seguridad y se filtró el **ID** con el dato **4624**, que es el de inicio de sesión. Esto no es necesario con el SIEM ya que el clasifica según sus registros los eventos y los muestras en una forma más fácil de administrar. Si se observa en la **Figura No 157** del SIEM el ID del Evento es el mismo, USERDATA4= 4624, pero la diferencia en el SIEM es que este si te da el **nombre de usuario**; en el caso de Windows lo que obtienes es el **GUID del usuario**.

En la forma convencional de administrar la seguridad y visibilidad es mucho más difícil identificar las amenazas y anomalías que están pasando en la red en tiempo real. Por lo general se tiene un servidor de LOG. Tal como se muestra en la **Figura No 159**.

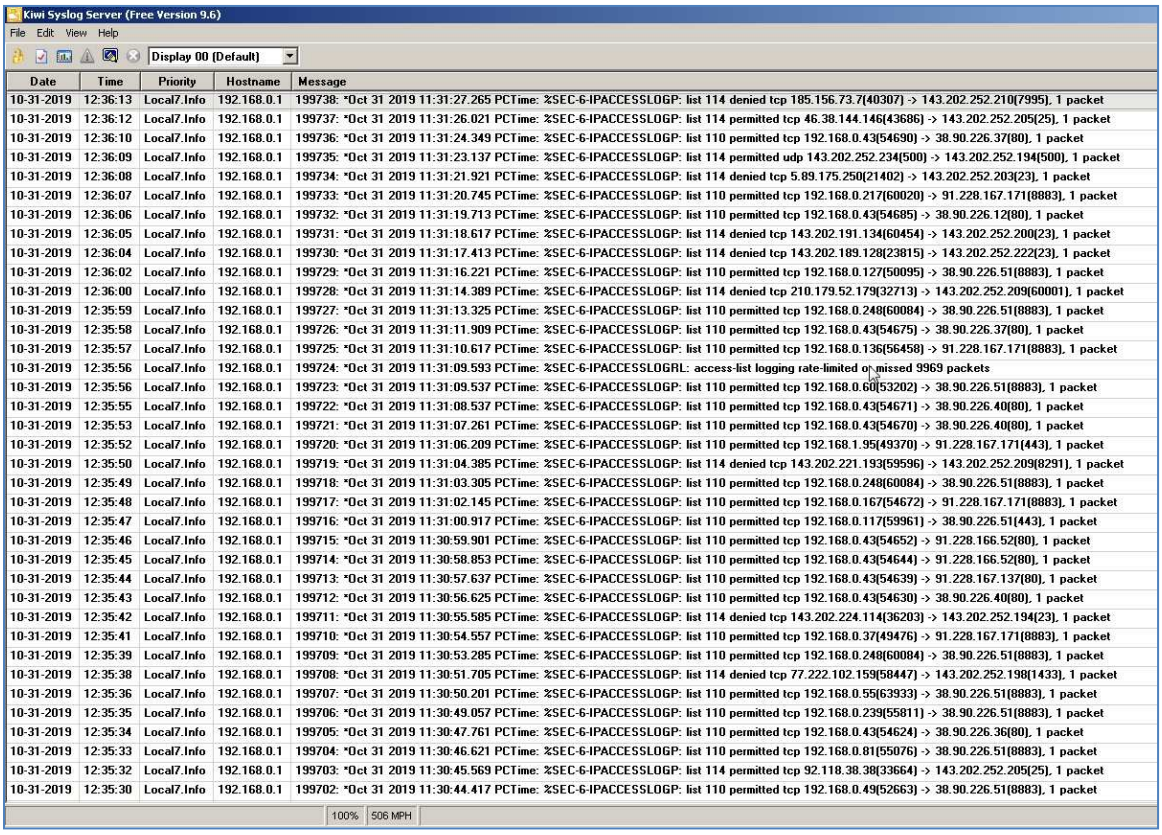


Figura No 159. Syslog del Router de pruebas (Captura de pantalla de equipo personal)

En la **Figura No 159** se muestra la dificultad de administrar cientos de miles de LOG. Si observamos el software de gestión en su parte inferior muestra la velocidad con la que se procesan y según el creador del mismo dice que es a 506MPH. Naturalmente esto significa que si el que está monitoreando la seguridad se distrae unos cuantos segundos existirán muy probables advertencias o errores que no podrán ver a tiempo. Otro problema que se enfrenta es que si la persona que está monitoreando se mueve de su posición de trabajo para ir al baño, comer o lo que sea no podrá a tiempo darse cuenta cuando un IP externo está intentando hacer una sesión ssh. A demás nadie le avisará lo que ocurrió y cuando se dé cuenta en la revisión que realice será muy tarde.

Lo mismo ocurre desde las interfaces de herramientas de gestión del UTM, si deseamos estar atentos a lo que ocurre e interpretar cada LOG será una labor casi imposible. Puesto que el volumen de LOG generados por día supera 1GB según los datos registrados por el SPLUNK que se instaló, Ver **Anexo A-3**.En la **Figura No 160** se muestra una imagen de los LOG del UTM.

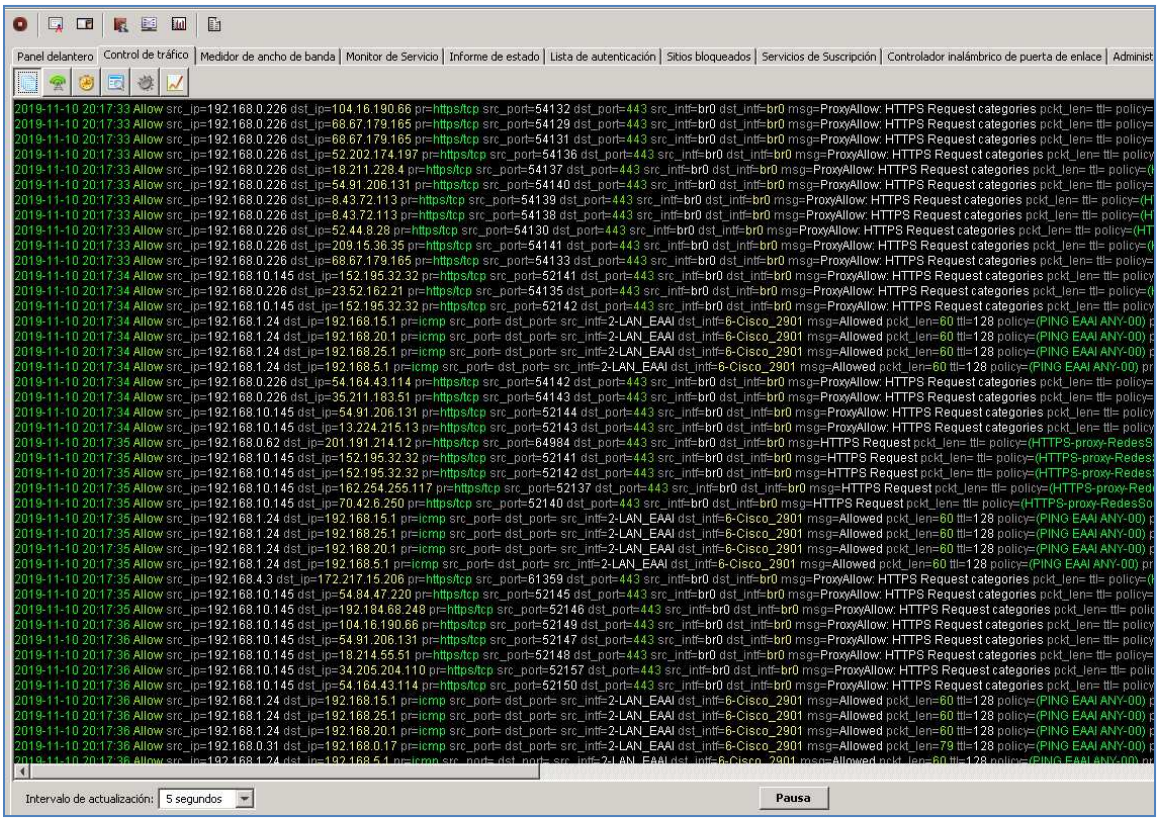


Figura No 160. Log generados por UTM (Captura de pantalla de equipo personal)

En la **Figura No 160** se observa un gran número de LOG que para poder entenderlos en tiempo real tendríamos que pausarlos y perder otro gran número. En los LOG de este equipo hay información clave de atacantes, tipos de ataques y otros elementos que son útiles para tomar medidas.

Todos estos elementos citados anteriormente son una pequeña muestra de las diferencias y grandes ventajas que genera un SIEM. En este caso OSSIM con un simple vistazo a los cuadros de mando conocemos todo lo que está pasando en la red. La **Figura No 161** lo ejemplifica.

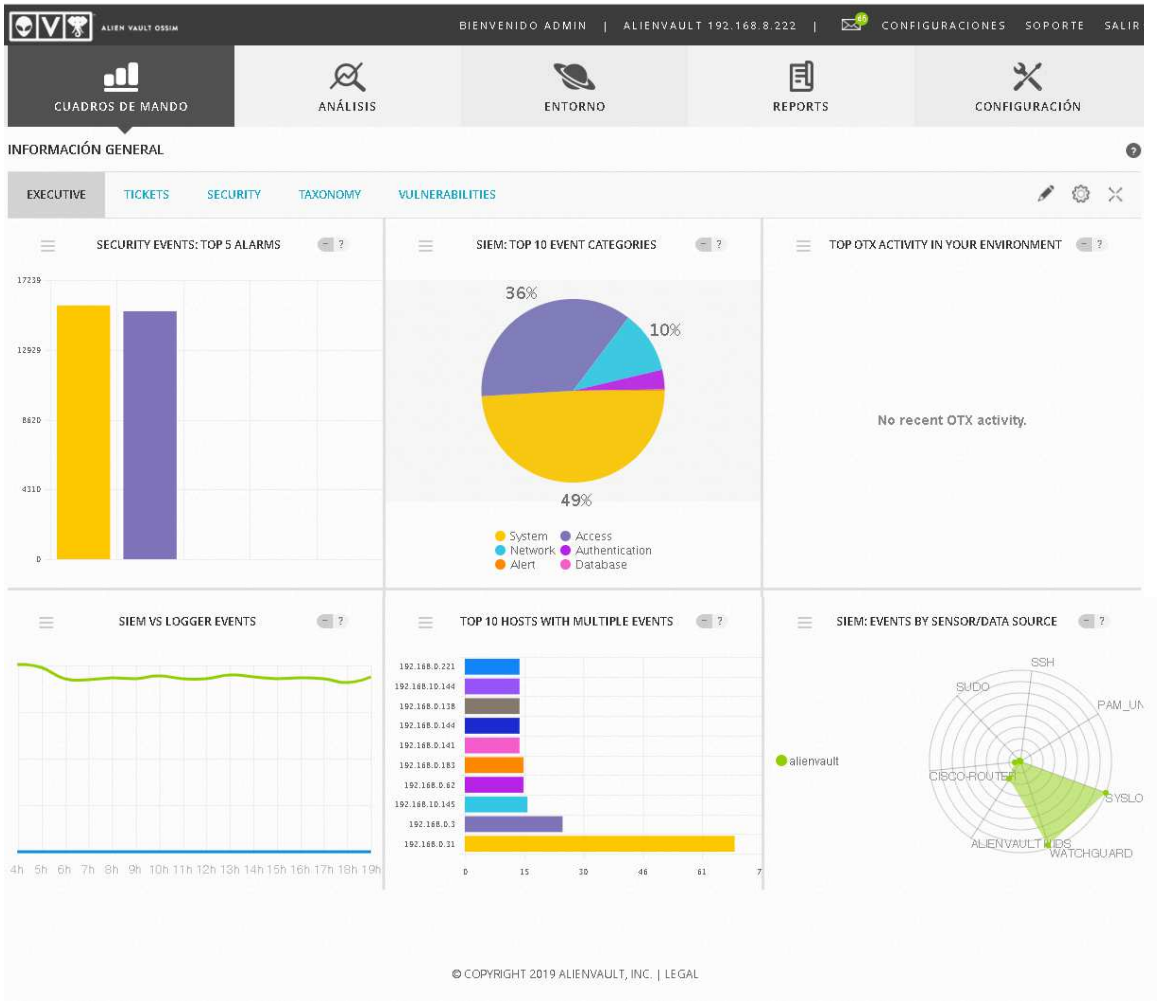


Figura No 161. Monitoreo centralizado de SIEM (Captura de pantalla de equipo personal)

En este cuadro de mando que muestra en la Figura No 161 se brinda una visión completa de la infraestructura de TI. Lo que con varios equipos nos costaría mucho tiempo y recursos humanos para entender y correlacionar todos los eventos se convierte en algo tan simple como un clic. Al observar la **Figura No 161** nos muestra la gráfica de **Eventos por Sensor o fuente de datos** ("EVENTS BY SENDOR/DATA SOURCE"), nos brinda una información de que equipo está produciendo más LOG y que también debemos estar atentos al cuadro superior llamado **10 Eventos por Categoría** ("10 EVENT CATEGORIES") que muestra las principales actividades detectadas por el SIEM. En solo este cuadro de mando adicional tenemos alarmas, actividad OTX y gráficos de los LOG generados.

9.2. AJUSTES DE MÓDULOS DE SERVICIO DE SIEM

Los ajustes que se pueden hacer a los módulos de servicio del SIEM tienen que ver con elementos como instalación de nuevos Plugin (en español complementos), asignación de valores a los activos, búsqueda de activos, escaneo de vulnerabilidades, creación de reglas, políticas y alertas. En este apartado haremos algunas demostraciones de elementos que podemos hacer. La siguiente imagen muestra cómo crear una política.

Para esto hay que ir a menú "CONFIGURACION", sub-menú "INFO. SOBRE AMENAZAS" y seleccionamos opción "POLITICA". En este punto hacemos clic en "Nuevo" en la parte de "Default policy group" (en español política de grupo por defecto). Ver **Figura No 162**.

Figura No 162. Creación de política en SIEM (Captura de pantalla de equipo personal)

En la **Figura No 163** se procede a configurar el nombre de la política en el campo "Nombre de la regla de la política". En la parte de abajo que dice "CONDICIONES DE LA POLÍTICA" son los elementos que vamos seleccionando en cada item de "CONDICIONES" y "CONSECUENCIAS". Por ejemplo el campo "ORIGEN" dice que es aplicable para cualquiera y el campo destino está en blanco.

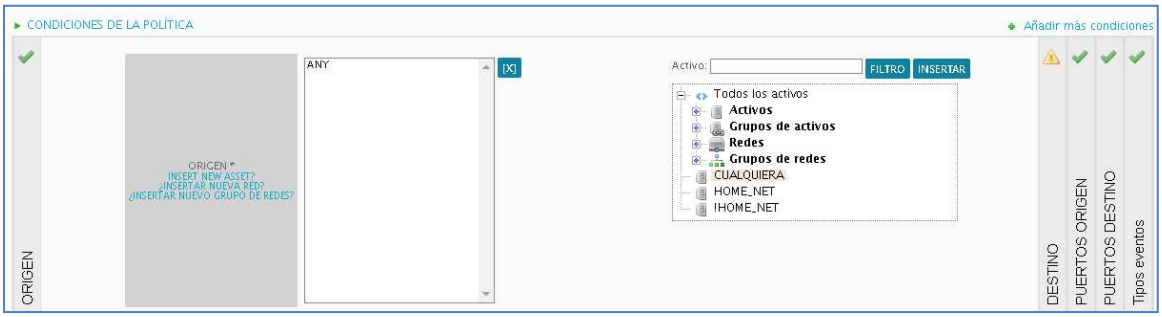


Figura No 163. Nombre de Política (Captura de pantalla de equipo personal)

En nuestro caso cambiamos el campo de Origen como se muestra en la **Figura No 164**. Al seleccionar el IP de AlienVault de la lista de las redes registradas.

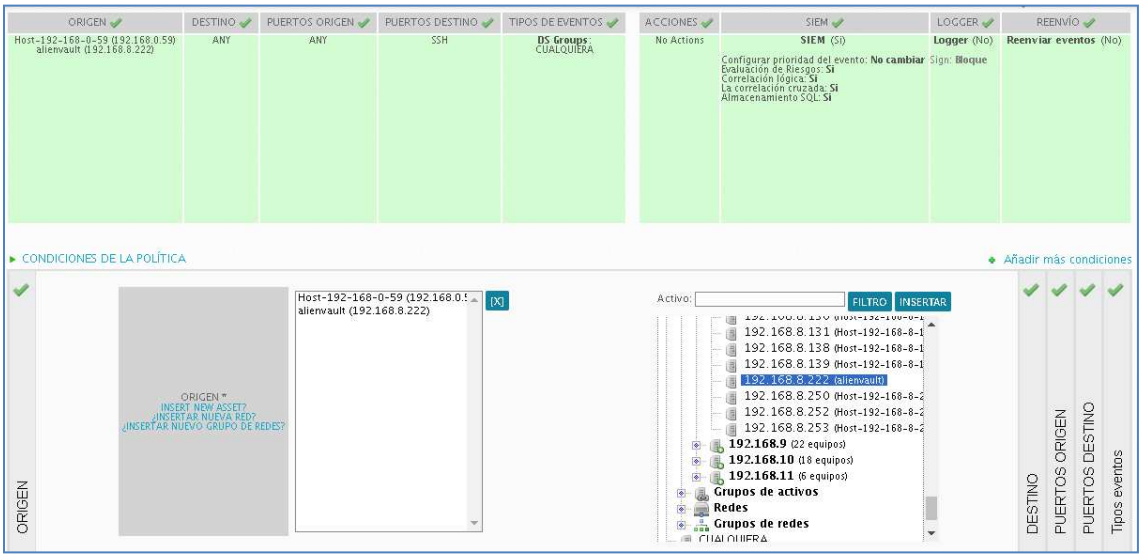


Figura No 164. Modificando campo Origen en la política (Captura de pantalla de equipo personal)

En condiciones en puerto destino cambiamos el puerto por el de SSH, TCP 22. Para eso hacemos clic en la pregunta "¿INSERTAR NUEVO GRUPO DE PUERTOS?". Tal como se observa en la **Figura No 165**.

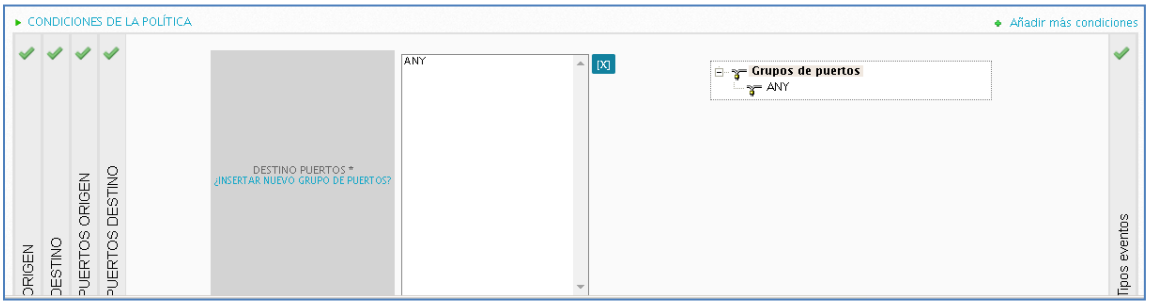


Figura No 165. Creando nuevo grupo de puertos (Captura de pantalla de equipo personal)

El resultado del clic es la siguiente imagen mostrada en la **Figura No 166** donde creamos el nuevo grupo de puerto.

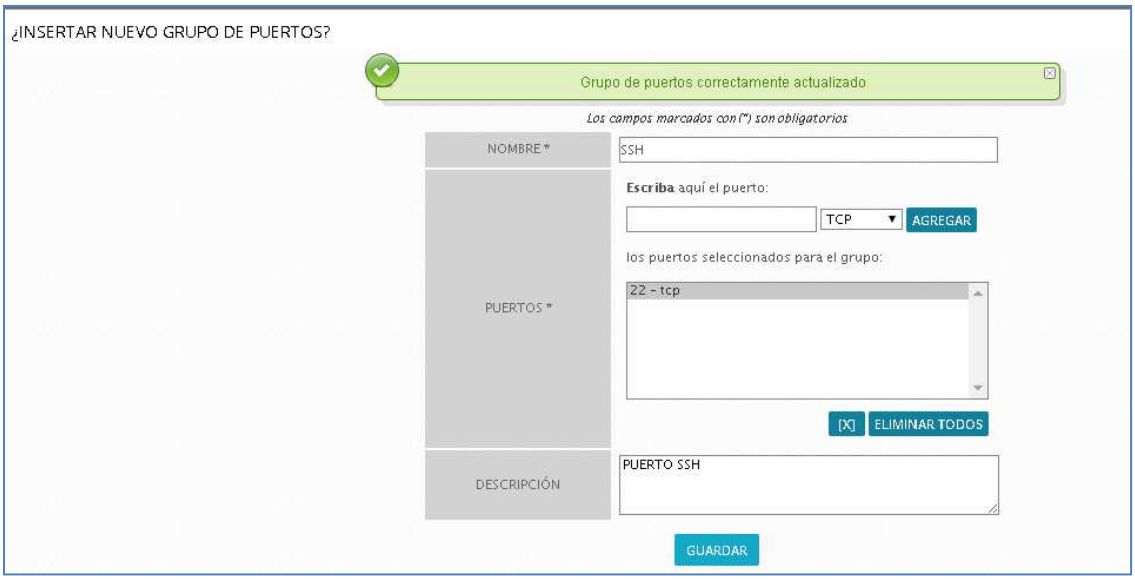


Figura No 166. Creación de grupo de puertos para SSH (Captura de pantalla de equipo personal)

En este caso en la **Figura No 166** muestra que escribimos el nombre y designamos el puerto TCP-22 para el servicio SSH, luego hacemos clic en "GUARDAR" para crear el SSH. Con el puerto creado solo lo agregamos tal y como se muestra en la **Figura No 167**.

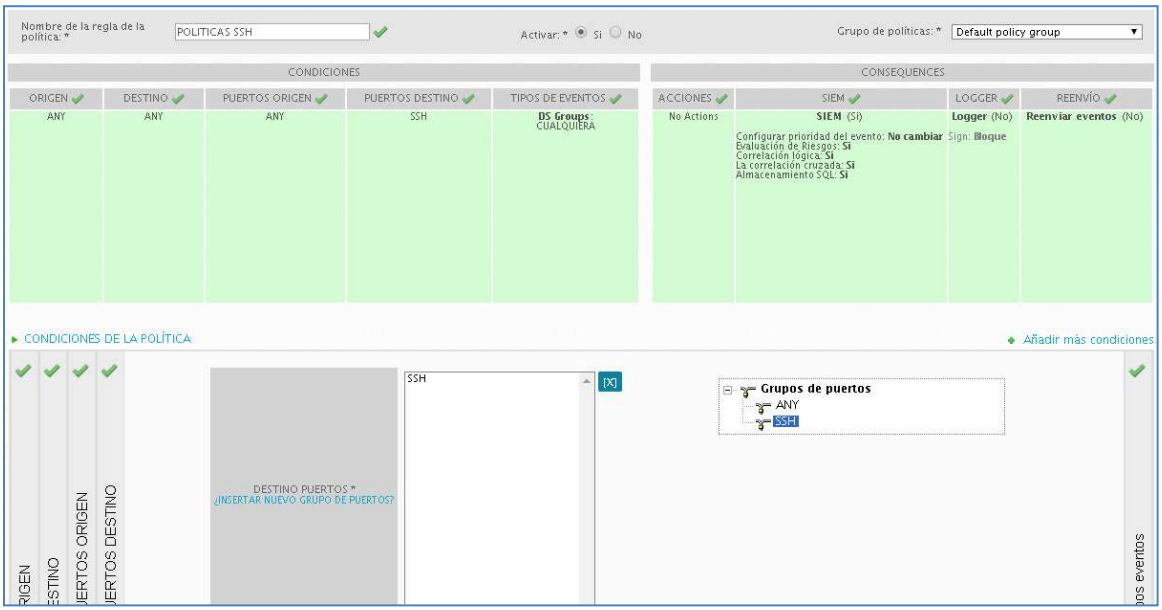


Figura No 167. Grupo de Puertos SSH agregado a puerto Destino (Captura de pantalla de equipo personal)

Ahora en la **Figura No 168** seleccionamos “Condiciones” en “Tipos de Eventos” hacemos clic en “INSTERTAR NUEVO GRUPO OD”. Esto con el fin de generar una política que mapee los eventos SSH Login Fail.

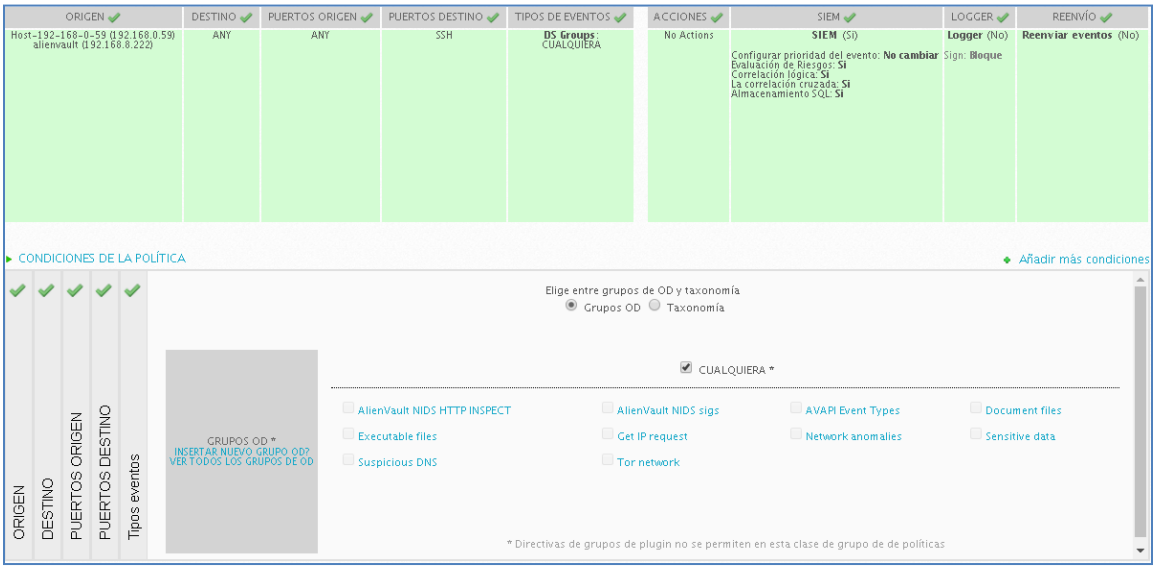


Figura No 168. Insertar grupo OD (Captura de pantalla de equipo personal)

Escribimos el nombre del Grupo, “FULL SSH SIN PASSWORD”, y su descripción. Realizamos búsquedas de Tipo de evento que contengan la palabra “password” y filtramos en esos eventos los que son por el servicio “sshd” y finalmente seleccionamos el “ORIGEN DE DATOS 4003”. Tal como se muestra en la **Figura No 169**.

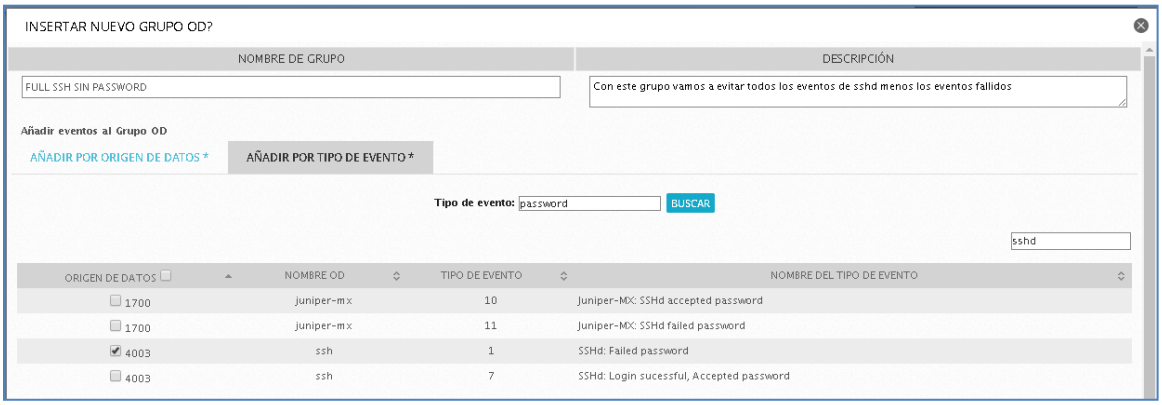


Figura No 169. Seleccionando evento SSH Fallido como grupo OD (Captura de pantalla de equipo personal)

Una vez actualizado la **Figura No 170** nos muestra el grupo ya creado y solo resta relacionarlo

Figura No 170. Grupo OD creado para SSH Fallido (Captura de pantalla de equipo personal)

Ahora solo hacemos en la Figura No 171 es hacer clic en "FULL SSH SIN PASSWORD" y se relaciona a la política que estamos creando.

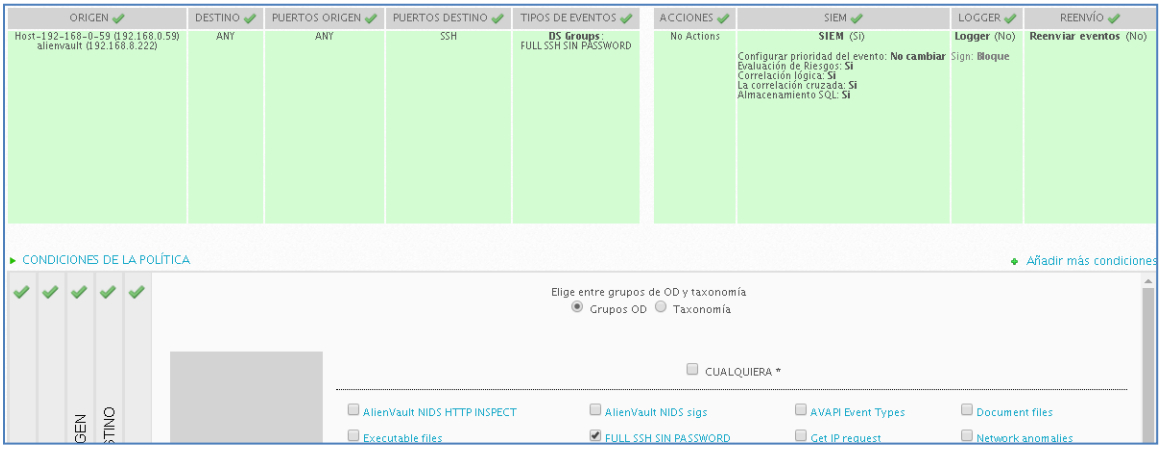


Figura No 171. Relacionando grupo OD a la política (Captura de pantalla de equipo personal)

Ahora solo guardamos y la política ya está creada tal como se muestra en la **Figura No 172**.

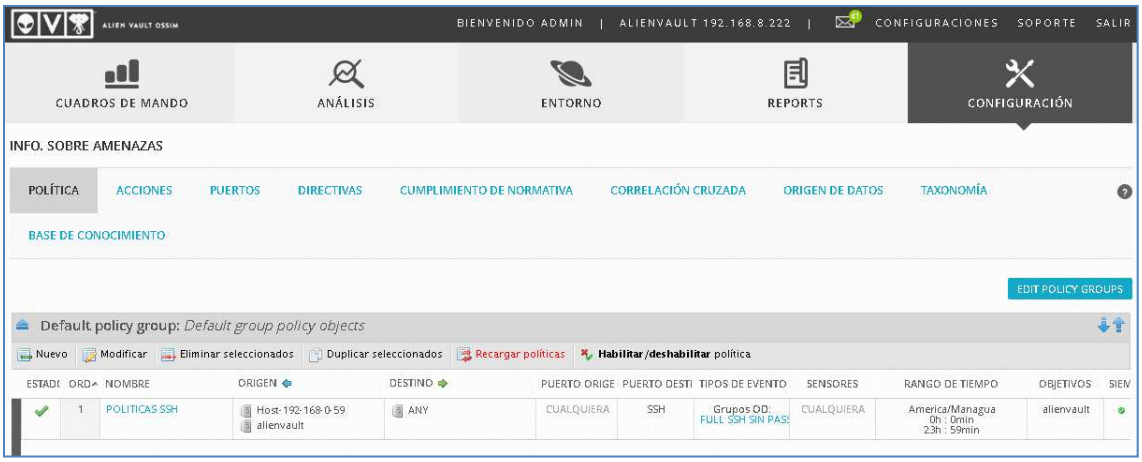


Figura No 172. Política SSH creada (Captura de pantalla de equipo personal)

Para los ajustes de los módulos del SIEM es muy importante que se lleve a cabo una búsqueda de activos con información de los sistemas operativos que posee. Para esto menú "ENTORNO", sub-menú "ASSET & GROUPS" (en español activos y grupos) seleccionamos la opción "ACTIVOS" y en el botón combinado "AÑADIR ACTIVOS" seleccionamos "Scan For New Assets" (en español búsqueda de nuevos activos), tal como se muestra en la **Figura No 173**.

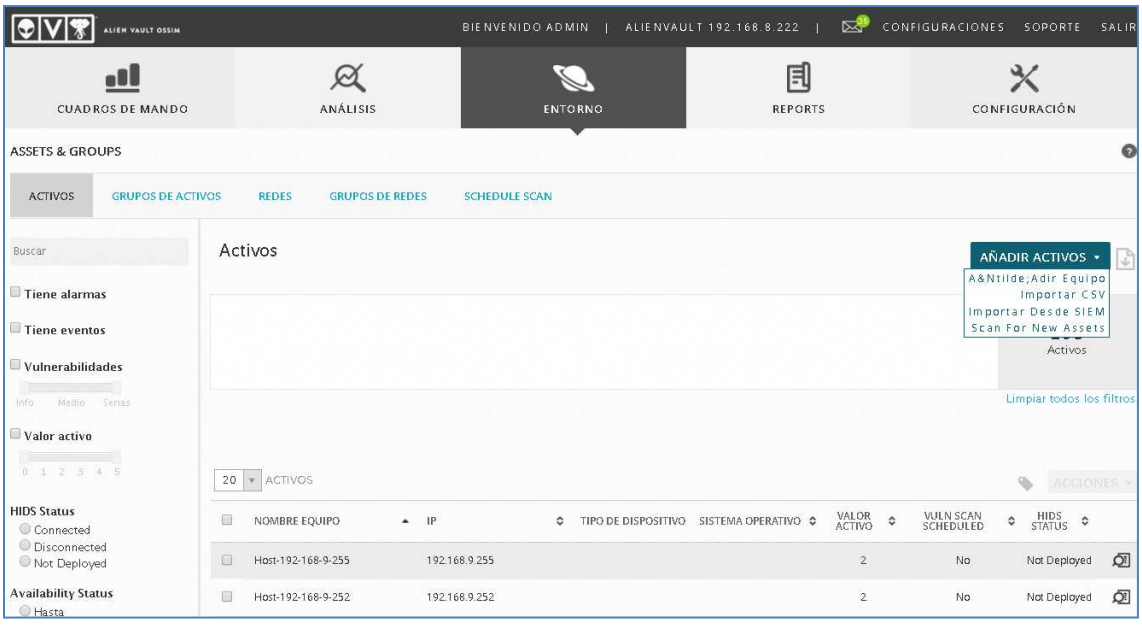


Figura No 173. Menú añadir activo (Captura de pantalla de equipo personal)

En este punto solo de la lista de activos seleccionamos la red y el IP que nos interesa. Tal como se observa en la Figura No 174.

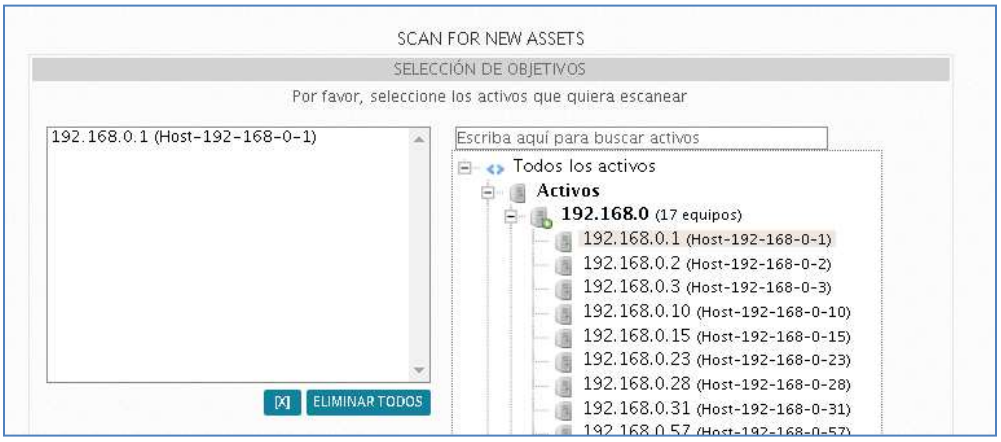


Figura No 174. Selección de IP de activo (Captura de pantalla de equipo personal)

En la configuración mas inferior mostrado en la **Figura No 175** se selecciona el sensor, tipo de escaneo, las opciones detectar sistema operativo y servicios. A demás la resolución de nombres de dominio (DNS)

Figura No 175. Configuración de escaneo de activo (Captura de pantalla de equipo personal)

Luego hacemos clic en "INICIAR ESCANEO".

Inicia el proceso de escaneo mostrado en la **Figura No 176**.

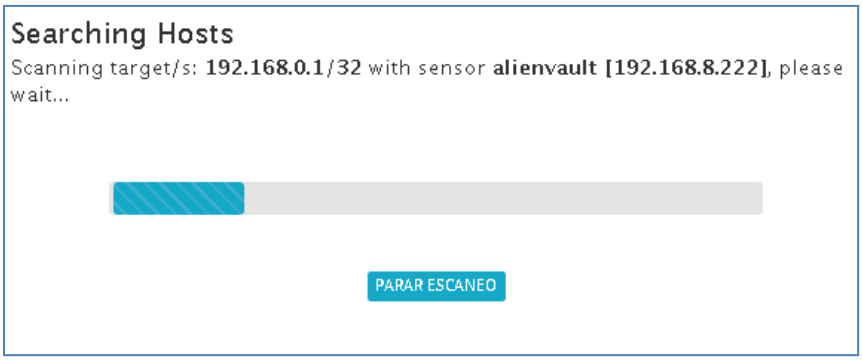


Figura No 176. Proceso de escaneo de activos indicado (Captura de pantalla de equipo personal)

Una vez finalizado nos da el resultado tal y como se muestra en la **Figura No 177**.

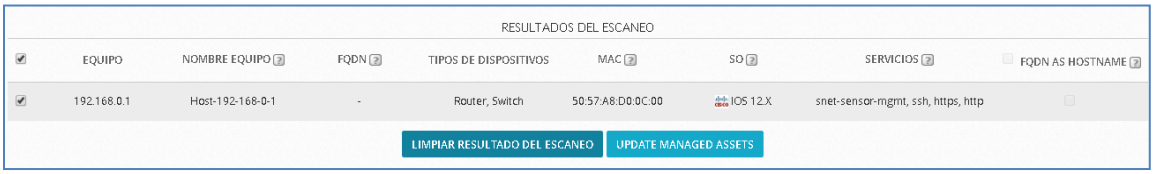


Figura No 177. Resultado de escaneo de activo (Captura de pantalla de equipo personal)

Ahora solo nos queda actualizar la información del activo. Para eso hacemos clic en "UPDATE MANAGED ASSETS" (en español actualizar activos administrados) de la **Figura No 177**. Como resultado nos aparecerán más elementos que llenar como los mostrados en la **Figura No 178**.

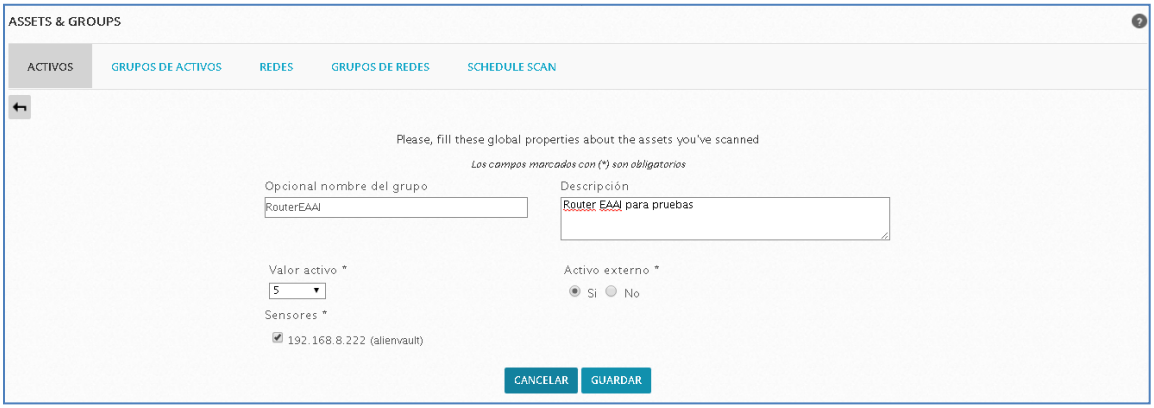


Figura No 178. Actualización de datos de activo (Captura de pantalla de equipo personal)

Lo más importante antes de guardar es establecer Valor activo. En este caso le damos la mayor importancia (campo va del 0 al 5) que es 5. Tal como se

muestra en la **Figura No 178**. Después de llenar nombre, valor y descripción guardamos. La Figura No 179 nos muestra el mensaje que indica que el activo fue actualizado correctamente.

Figura No 179. Actualización de activo satisfactoria (Captura de pantalla de equipo personal)

Un elemento imprescindible para configurar en el SIEM es la realización de análisis de vulnerabilidades. Esto es de vital importancia porque una vez escaneado el activo (Computador, Servidor o Dispositivo de Red) el SIEM proporcionará las alertas requeridas en los cuadros de mando con el activo ya escaneado. Las siguientes imágenes mostraran el proceso de escaneo de vulnerabilidades.

Lo primero es ir a menú "ENTORNO" y seleccionar sub-menú "VULNERABILIDADES". Luego hacer clic en "TRABAJOS DE ESCANEO" y presionar botón "NUEVO TRABAJO DE ESCANEO". Ver **Figura No 180**.

Figura No 180. Trabajo de escaneo de vulnerabilidades (Captura de pantalla de equipo personal)

En el asistente de nuevo trabajo de escaneo ("CREATE SCAN JOB", en español crear trabajo de escaneo) mostrado en la **Figura No 181** seleccionamos los host a escanear.

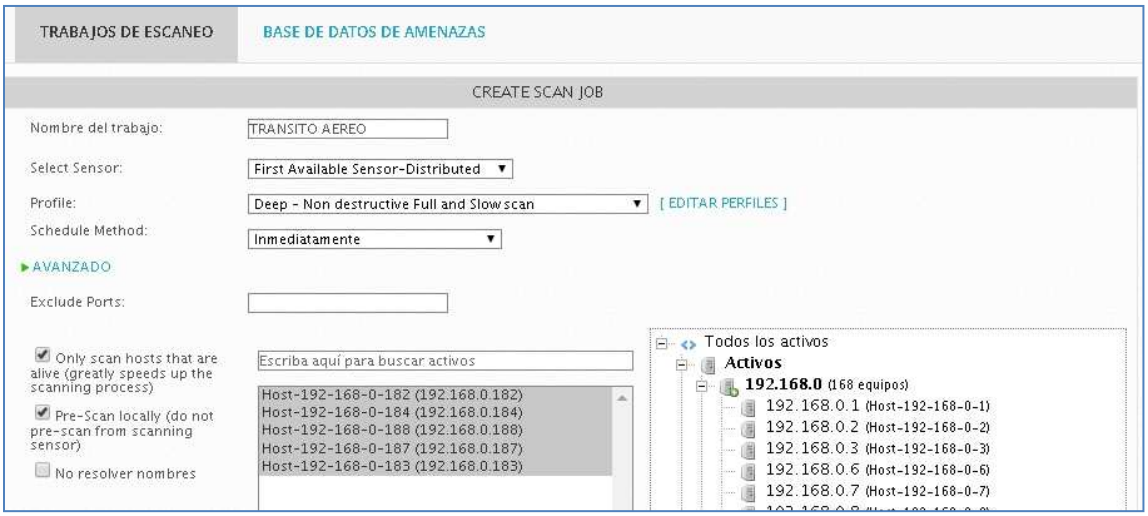


Figura No 181. Configuración de nuevo trabajo de escaneo (Captura de pantalla de equipo personal)

Más abajo en el asistente nos muestra en la **Figura No 182** que los equipos están visibles para realizar escaneo y hacemos clic en botón "GUARDAR".

Figura No 182. Guardando e iniciando escaneo de vulnerabilidades (Captura de pantalla de equipo personal)

En la **Figura No 183** muestra que el trabajo ya está en lista para iniciar su ejecución.

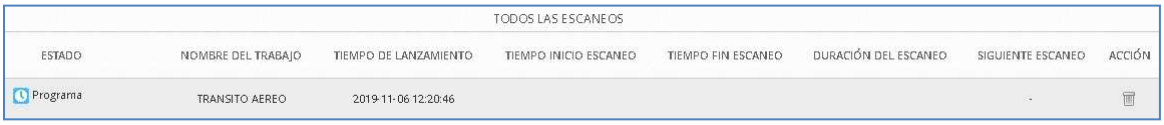


Figura No 183. Trabajo de escaneo en espera de ejecución inmediata (Captura de pantalla de equipo personal)

En la Figura No 184 muestra el trabajo que creamos en ejecución y un segundo trabajo creado posteriormente. . Como podemos observar que ambos trabajo están ejecutándose en paralelo.

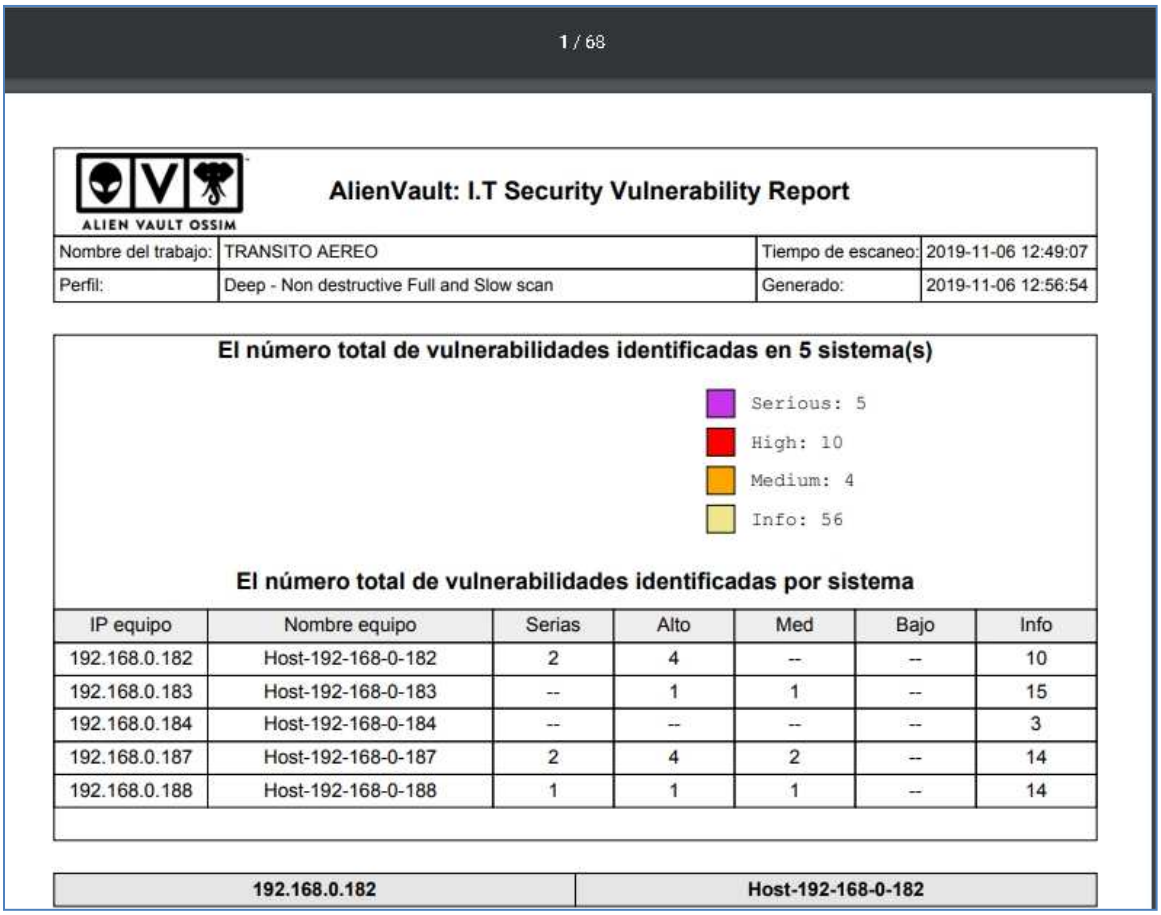
Figura No 184. Progreso de escaneo de vulnerabilidades (Captura de pantalla de equipo personal)

Una vez que se completan los trabajos en la **Figura No 185** se brinda un resumen de los mismos.

Figura No 185. Resumen de escaneo de vulnerabilidades (Captura de pantalla de equipo personal)

En la **Figura No 185** podemos ver que existe un lugar denominado "**ACCIÓN**" donde localizamos varios iconos que nos permiten la exportación o visualización del informe en distintos formatos (php, html, pdf, xls).

A continuación en la **Figura No 186** mostramos un reporte general del trabajo denominado "TRANSITO AEREO", donde se clasifican por IP las generalidades encontradas en: serias, altas, medias, baja e información.



1 / 68

ALIEN VAULT OSSIM

AlienVault: I.T Security Vulnerability Report

Nombre del trabajo:	TRANSITO AEREO	Tiempo de escaneo:	2019-11-06 12:49:07
Perfil:	Deep - Non destructive Full and Slow scan	Generado:	2019-11-06 12:56:54

El número total de vulnerabilidades identificadas en 5 sistema(s)

Serious: 5
High: 10
Medium: 4
Info: 56

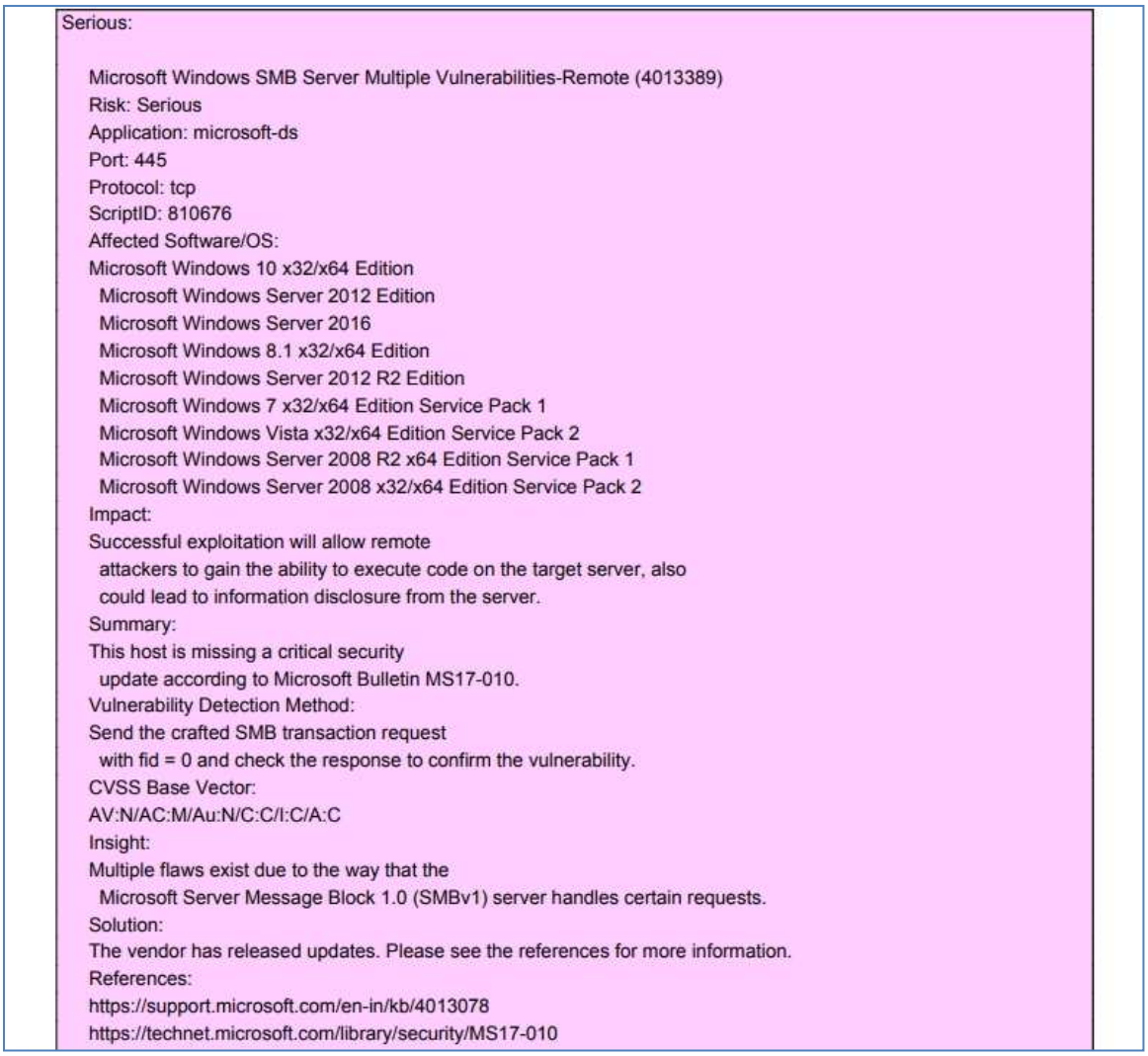
El número total de vulnerabilidades identificadas por sistema

IP equipo	Nombre equipo	Serias	Alto	Med	Bajo	Info
192.168.0.182	Host-192-168-0-182	2	4	--	--	10
192.168.0.183	Host-192-168-0-183	--	1	1	--	15
192.168.0.184	Host-192-168-0-184	--	--	--	--	3
192.168.0.187	Host-192-168-0-187	2	4	2	--	14
192.168.0.188	Host-192-168-0-188	1	1	1	--	14

192.168.0.182	Host-192-168-0-182

Figura No 186. Reporte de trabajo para TRANSITO AEREO (Captura de pantalla de equipo personal)

La **Figura No 187** muestra una porción del reporte que dice: Se ha detectado en uno de los equipos una vulnerabilidad en el protocolo Samba (SMB), brinda la información de los tipos de sistemas operativos afectados. Nos Informa la existencia del boletín de Microsoft MS-17010 donde se recomienda la actualización del producto por medio de un parche. Para esto nos da dos link el https://support.microsoft.com/en-in/kb/4013078 y el https://technet.microsoft.com/library/security/MS170-10.



Serious:

Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)
Risk: Serious
Application: microsoft-ds
Port: 445
Protocol: tcp
ScriptID: 810676
Affected Software/OS:
Microsoft Windows 10 x32/x64 Edition
Microsoft Windows Server 2012 Edition
Microsoft Windows Server 2016
Microsoft Windows 8.1 x32/x64 Edition
Microsoft Windows Server 2012 R2 Edition
Microsoft Windows 7 x32/x64 Edition Service Pack 1
Microsoft Windows Vista x32/x64 Edition Service Pack 2
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2
Impact:
Successful exploitation will allow remote
attackers to gain the ability to execute code on the target server, also
could lead to information disclosure from the server.
Summary:
This host is missing a critical security
update according to Microsoft Bulletin MS17-010.
Vulnerability Detection Method:
Send the crafted SMB transaction request
with fid = 0 and check the response to confirm the vulnerability.
CVSS Base Vector:
AV:N/AC:M/Au:N/C:C/I:C/A:C
Insight:
Multiple flaws exist due to the way that the
Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.
Solution:
The vendor has released updates. Please see the references for more information.
References:
https://support.microsoft.com/en-in/kb/4013078
https://technet.microsoft.com/library/security/MS17-010

Figura No 187. Porción de reporte de vulnerabilidad (Captura de pantalla de equipo personal)

Al explorar el link https://support.microsoft.com/en-in/kb/4013078 mostrado en la **Figura No 188** nos brinda en detalle el parche e información del boletín que lo recomienda. Como se observa la vulnerabilidad es permitir por medio de samba la ejecución de código remoto por un atacante.

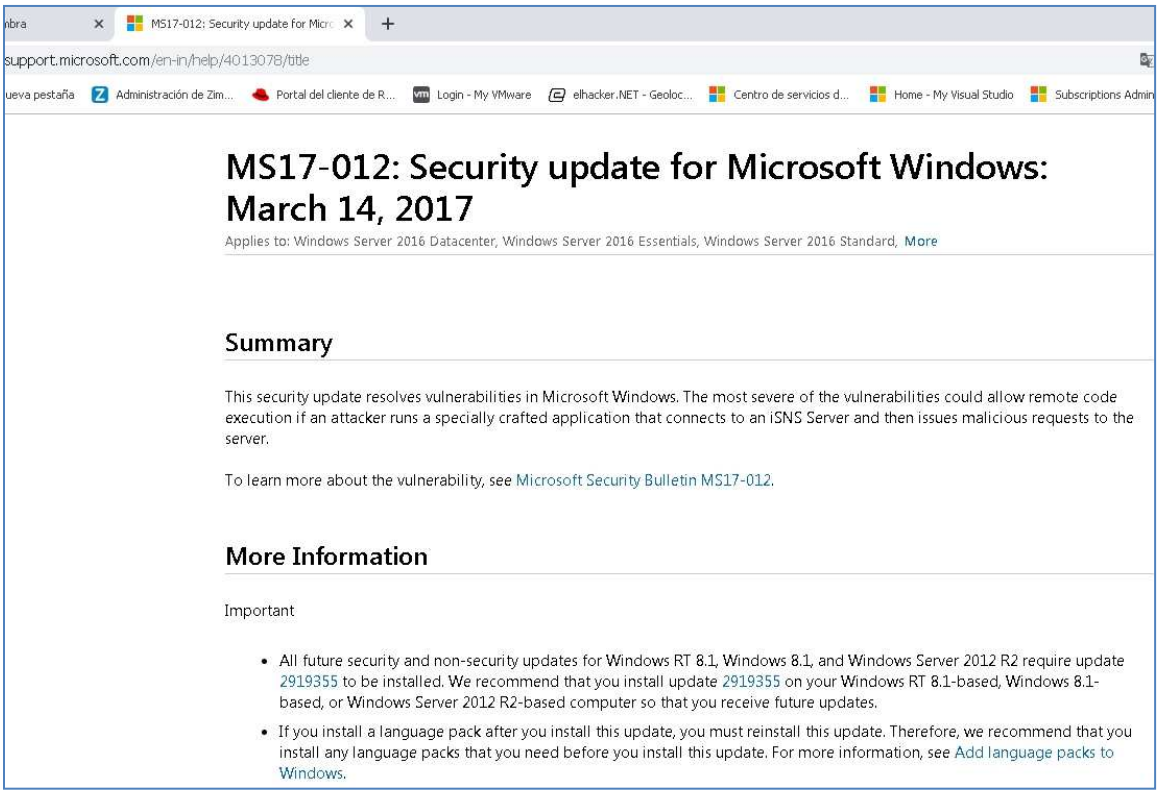


Figura No 188. Detalle de vulnerabilidad encontrada (Captura de pantalla de equipo personal)

La **Figura No 189** brinda ejemplo de uno de los archivos a descargar para una versión como el caso de Windows vista

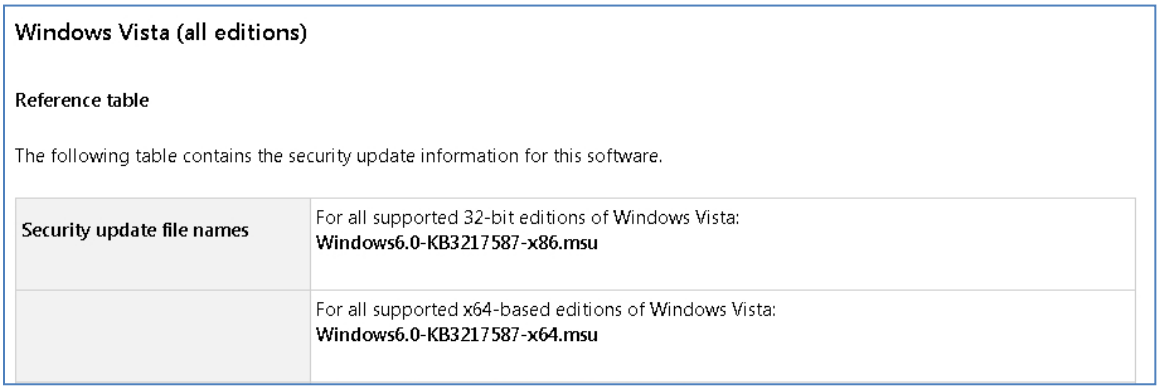


Figura No 189. Parche de seguridad a instalar (Captura de pantalla de equipo personal)

Ahora a niveles del menú "CUADROS DE MANDO" podemos ir al sub-menú "INFORMACIÓN GENERAL" y seleccionar la opción "VULNERABILITIES" (en español vulnerabilidades). Tal como se muestra en la **Figura No 190** brinda un resumen de todas las vulnerabilidades que han sido escaneadas en el sistema.

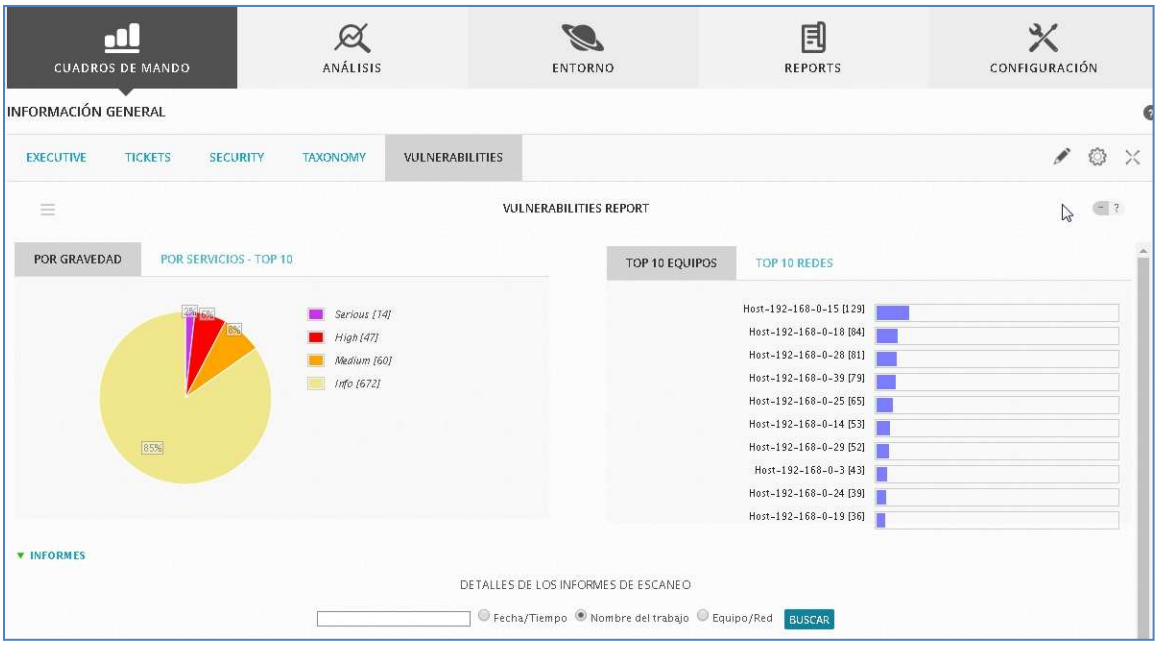


Figura No 190. Cuadro de mando de vulnerabilidades (Captura de pantalla de equipo personal)

En el mismo cuadro de mando más en su parte inferior encontramos detalle de todos los trabajos realizados y nos permite ver las vulnerabilidades en detalle. Además podemos exportar el informe con cualquier formato permitido (html, xls, pdf), tal como se muestra en la **Figura No 191**.

Figura No 191. Opciones de exportar reporte de vulnerabilidades (Captura de pantalla de equipo personal)

9.3. REPORTES DE SIEM

La **Figura No 192** muestra la reportaría del SIEM OSSIM. Brinda reportes de suma importancia para nuestra toma de decisiones. Para acceder a estos recursos hay que ir al menú "REPORTS" (en español reportes).

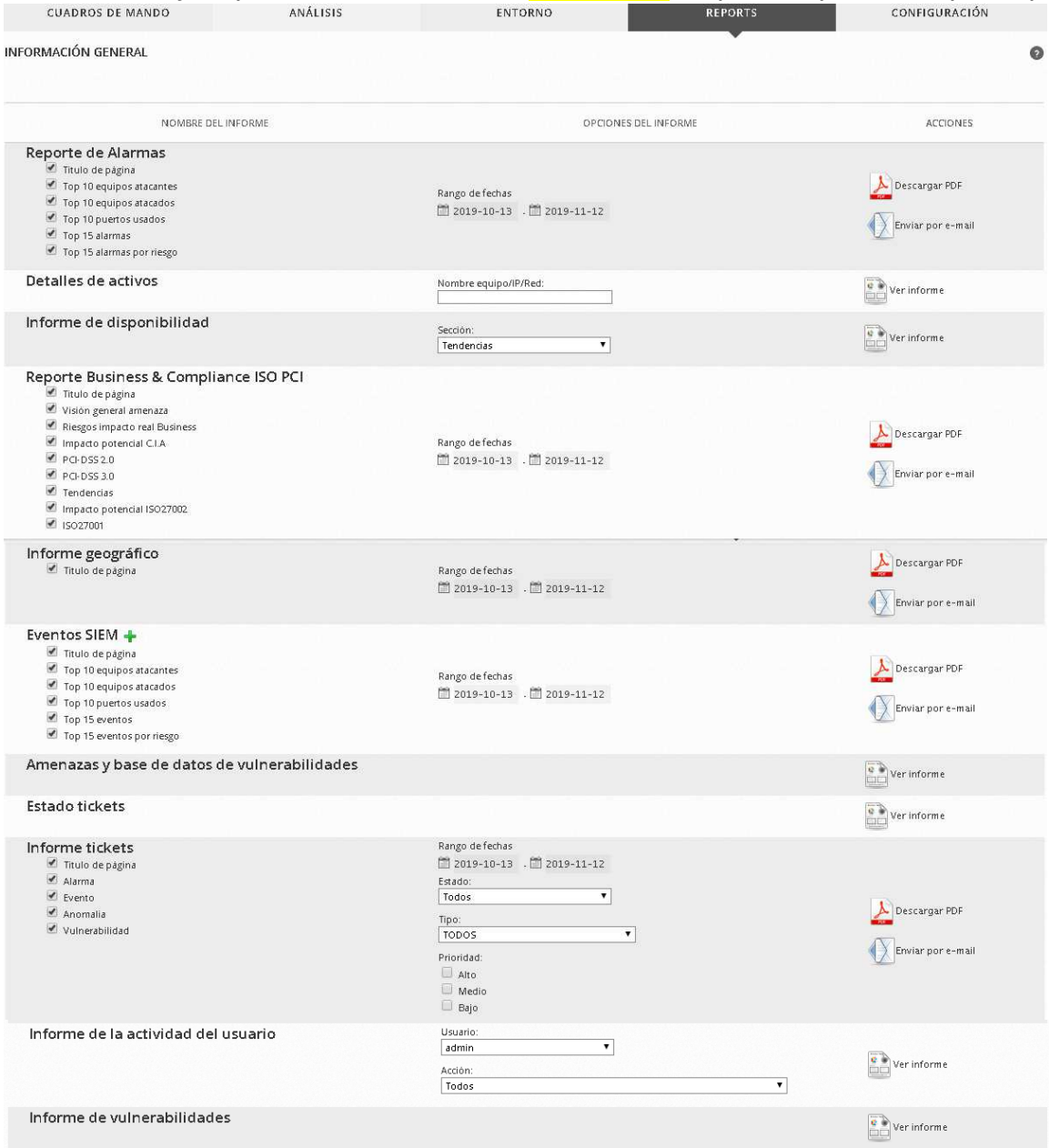


Figura No 192. Reportes de SIEM OSSIM (Captura de pantalla de equipo personal)

Listado de Informes de OSSIM

En la **Figura No 192** mostrada en la página anterior denominada Reportes de SIEM OSSIM ofrece un total de 11 informes, estos son:

- **Reporte de Alarmas:** Brinda información de las principales alarmas generadas en el sistema. Tal como equipos atacantes, equipos atacados, puertos más usados, Listado de las alarmas y sus ocurrencias.
- **Detalles de Activos:** Brinda información detallada de los activos que han sido escaneados. Tal como listado de vulnerabilidades, alarmas, eventos, disponibilidad, servicios, software, grupos a los que pertenece y notas.
- **Informa de disponibilidad:** Muestra un resumen completo de la disponibilidad de los equipos. Para esto se hace uso de un asistente que nos permite seleccionar el periodo de tiempo y equipos.
- **Resporte Business & Compliance ISO PCI**: Genera un reporte de cumplimento de acuerdo a los elementos seleccionados o normas tal como ISO o PCI. En este informe se muestran los vectores de ataque y el impacto que generan a la organización de ser logrados.
- **Informe geográfico:** Nos da detalle de todos los eventos de ataques recibidos a nivel mundial a nuestra infraestructura.
- **Eventos SIEM:** Nos da un detalle general de los host que producen más ataques, equipos atacados, eventos más críticos con sus ocurrencias
- **Amenazas y base de datos de vulnerabilidades:** Muestra información de todas las amenazas almacenadas en la base de datos de vulnerabilidades.
- **Estado de tickets:** Brinda reporte del estado de los ticketes que abrimos cuando ocurre un evento.
- **Informe ticketes:** Lista todos los ticketes abiertos
- **Informe de la actividad del usuario:** Muestra la información de los usuarios logados al SIEM.
- **Informe de vulnerabilidades:** Lista informe de vulnerabilidades de los equipos que han sido escaneados

A continuación se presentaran ejemplos de algunos informes generados. El primero que se mostrará es el "Informe de Alarmas". Para esto seleccionaremos todos los elementos que se permiten para este reporte y lo recibiremos vía correo. Tal como se observa en la **Figura No 193.**

Figura No 193. Reporte de Alarmas (Captura de pantalla de equipo personal)

En este caso le damos el correo dmvega@eaai.com.ni , el cual también está configurado como dirección de envío en OSSIM.

El proceso inicia una vez que le damos clic en el botón "ENVIAR". Ver **Figura No 194**.

Figura No 194. Generando solicitud por correo de informe de alarmas (Captura de pantalla de equipo personal)

Una vez generado el reporte tal como muestra la **Figura No 195** se muestra un mensaje en pantalla diciendo que ya fue enviado.

Figura No 195. Informe PDF enviado por email (Captura de pantalla de equipo personal)

Si se revisa el correo se observa en la **Figura No 196** ya el reporte está en la bandeja de entrada.

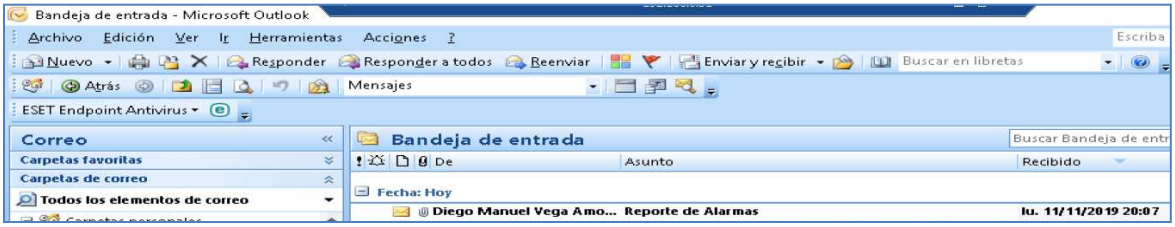


Figura No 196. Correo con Reporte de SIEM en pdf (Captura de pantalla de equipo personal)

La **Figura No 197** muestra el correo abierto y se observa que el contenido es un PDF con el informe de las alarmas.

Figura No 197. Documento pdf en correo con reporte de alarma (Captura de pantalla de equipo personal)

Este al igual que los otros informes tiene su portada. Tal y como se muestra en la **Figura No 198,** donde muestra fecha de reporte, periodo de reporte y la cantidad de activos seleccionados.

Figura No 198. Portada de reporte de alarmas en pdf (Captura de pantalla de equipo personal)

En la **Figura No 199** de una página del reporte muestra el resumen de las ocurrencias y atacantes.

Figura No 199. Reporte de alarmas- equipos atacantes (Captura de pantalla de equipo personal)

La **Figura No 200** muestra el detalle de equipos atacados. En este caso se observan los 10 más altos en ocurrencias.

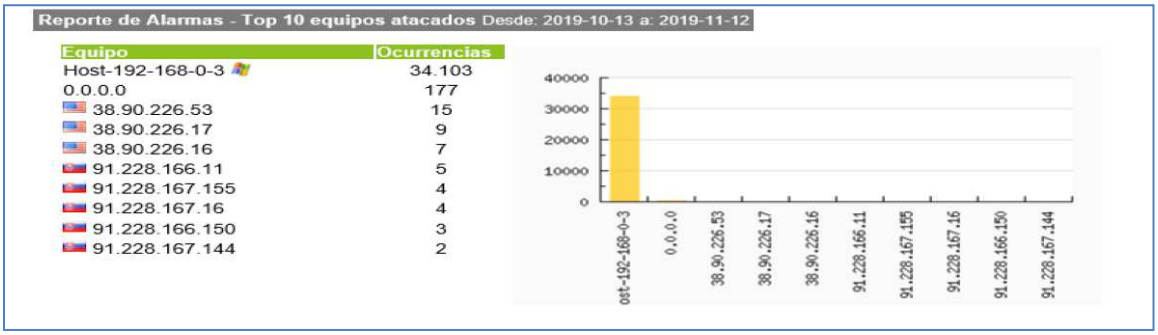


Figura No 200. Equipos atacados (Captura de pantalla de equipo personal)

En la **Figura No 201** se muestran los servicios más usados.

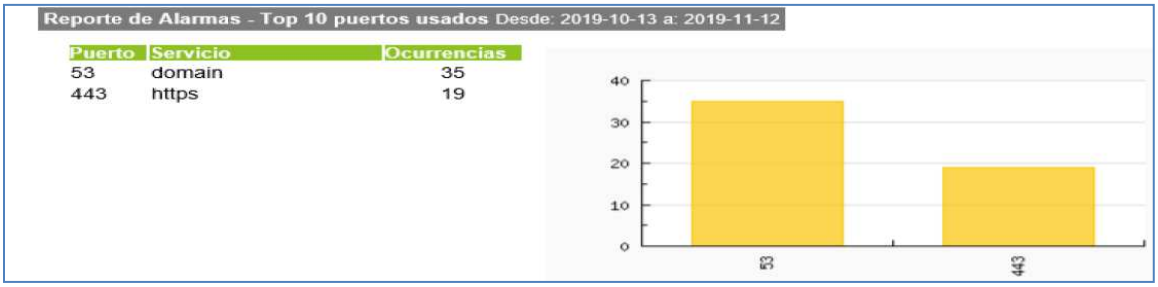


Figura No 201. Reporte de servicios más usados (Captura de pantalla de equipo personal)

En la siguiente parte del informe en la **Figura No 202** se muestra la distribución de las alarmas. Podemos observar que se describen las quince alarmas más activas con las frecuencias de sus ocurrencias. A demás se ofrece un diagrama de tipo pastel donde se muestra la proporción de cada alarma.

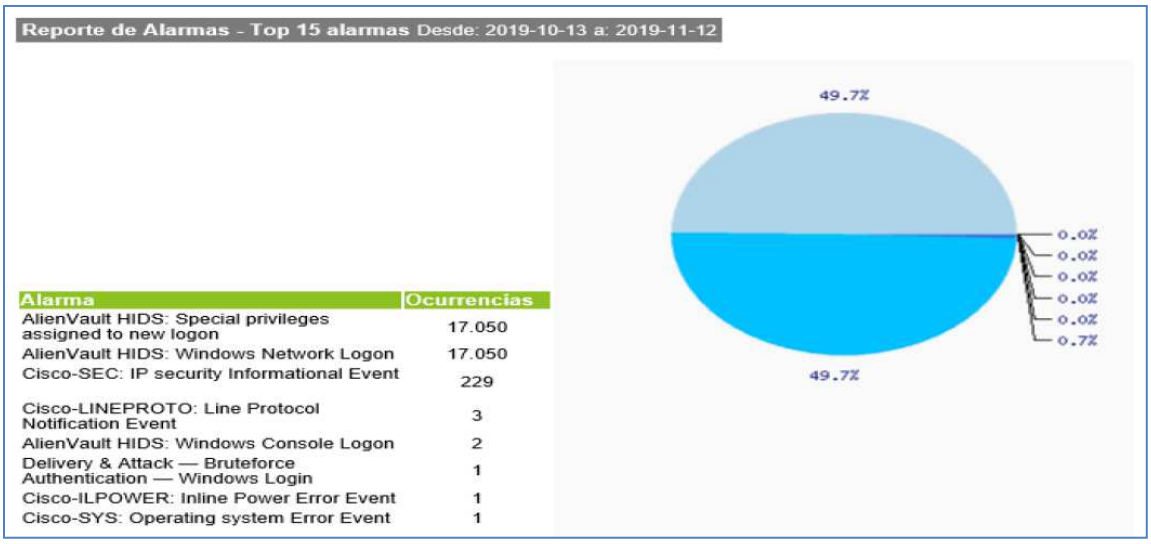


Figura No 202. Reporte de alarmas (Captura de pantalla de equipo personal)

Con este informe que se amostrado por secciones se puede dar una idea de los principales elementos que están registrando alarmas en nuestra red. Cabe mencionar que los datos que se han generado son de pocos activos.

En el caso que deseemos un reporte visual del detalle de los activos generamos el reporte "Detalles de activos". Tal como se muestra en la **Figura No 203**.

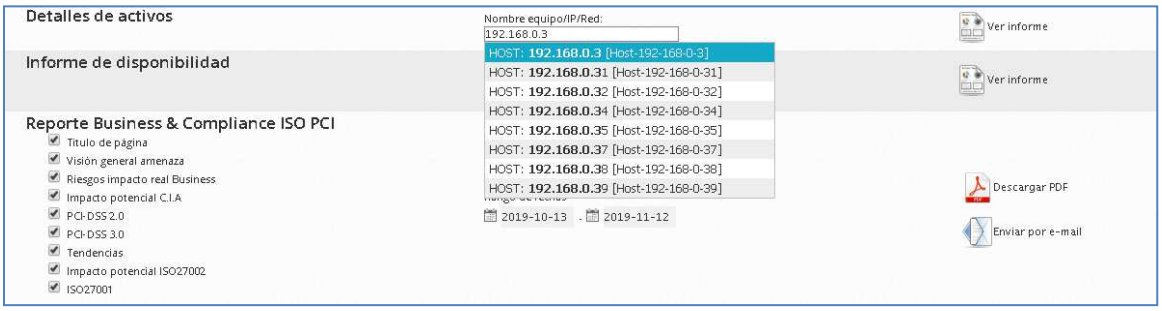


Figura No 203. Seleccionando activo para reporte (Captura de pantalla de equipo personal)

Al seleccionar el Host con IP 192.168.0.3 hacemos clic en "ver informe". Como resultado nos muestra en la **Figura No 204** toda la información referida al activo en una especie de cuadro de mando pero dentro del menú "ENTORNO", sub-menú "ASSET & GROUPS" (en español activos y grupos) y opción "ACTIVOS".

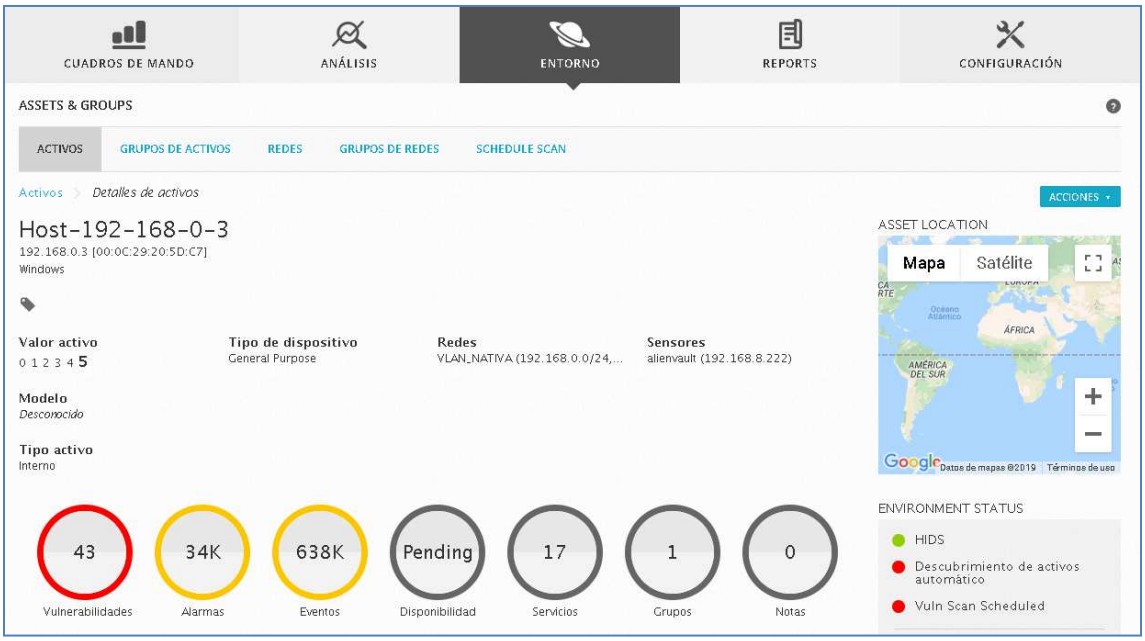


Figura No 204. Información del activo generada por reporte (Captura de pantalla de equipo personal)

En la **Figura No 204** se observa el detalle general de vulnerabilidades, alarmas, eventos, disponibilidad, servicios, grupos y notas. A cada círculo se le puede hacer clic para ver la información. En este punto hacemos clic a "Vulnerabilidades". Nos muestra en la **Figura No 205** las "VULNERABILIDADES" listadas del activo.

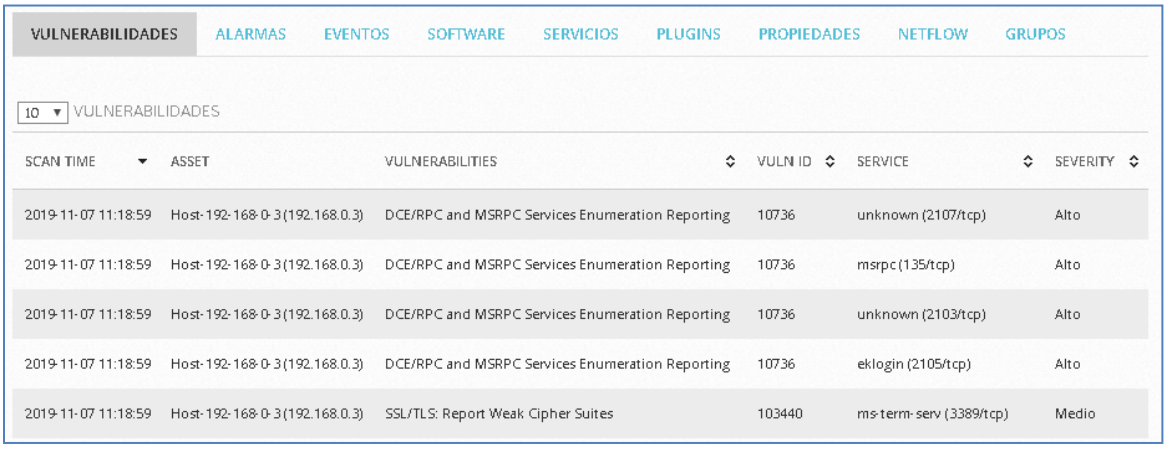


Figura No 205. Vulnerabilidades del activo (Captura de pantalla de equipo personal)

Si hacemos clic en "EVENTOS" se muestra la **Figura No 206** donde se listan todos los eventos que han ocurrido en el activo. Tal como se muestra a continuación.

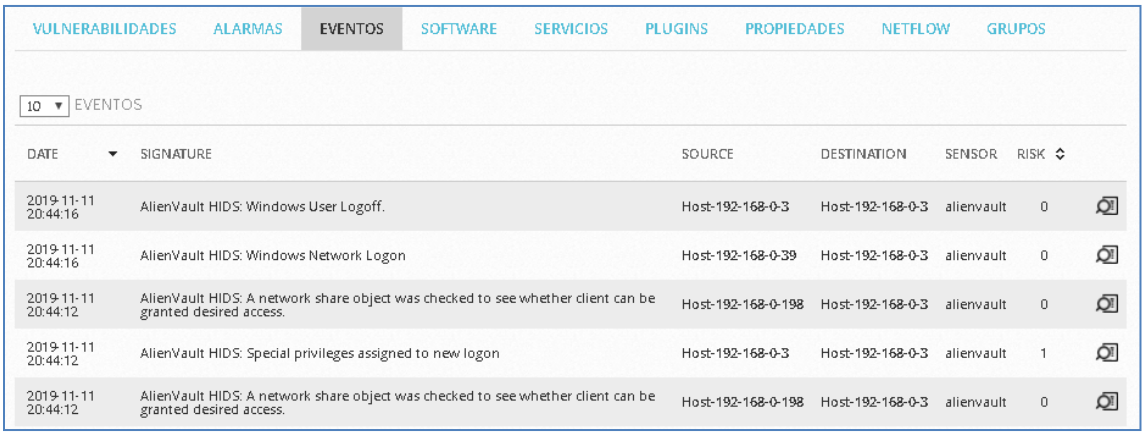


Figura No 206. Eventos del activo (Captura de pantalla de equipo personal)

En la **Figura No 207** "SOFTWARE" vemos todo el inventario que los escaneos han enviado.

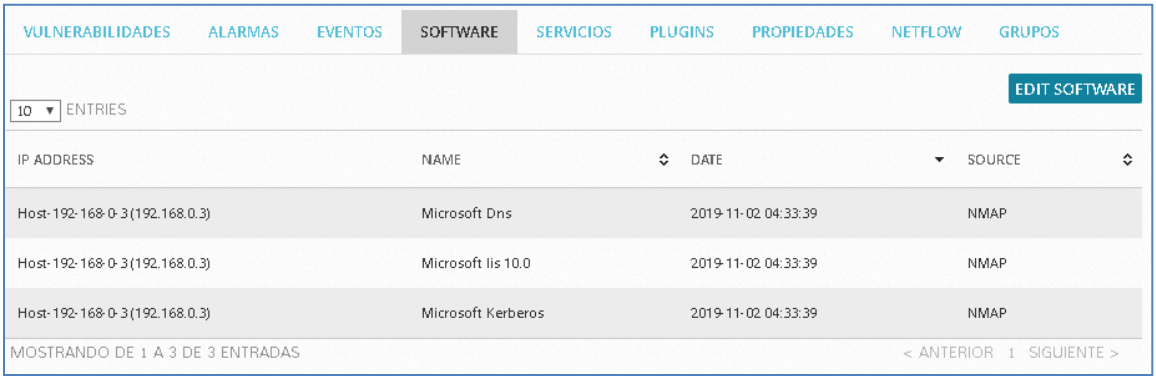


Figura No 207. Software listado del activo (Captura de pantalla de equipo personal)

Con la información mostrada en la **Figura No 207** podemos darnos cuenta de las principales funciones que presta este servidor. En este caso es un servidor DNS, Web y de Autenticación (Controlador de Dominio, Kerberos está activo). La herramienta usada para el descubrimiento por el SIEM fue NMAP. Si seleccionamos los "SERVICIO" podemos observar una lista detallada de servicios del sistema operativo. Tal y como se muestra en la **Figura No 208**.

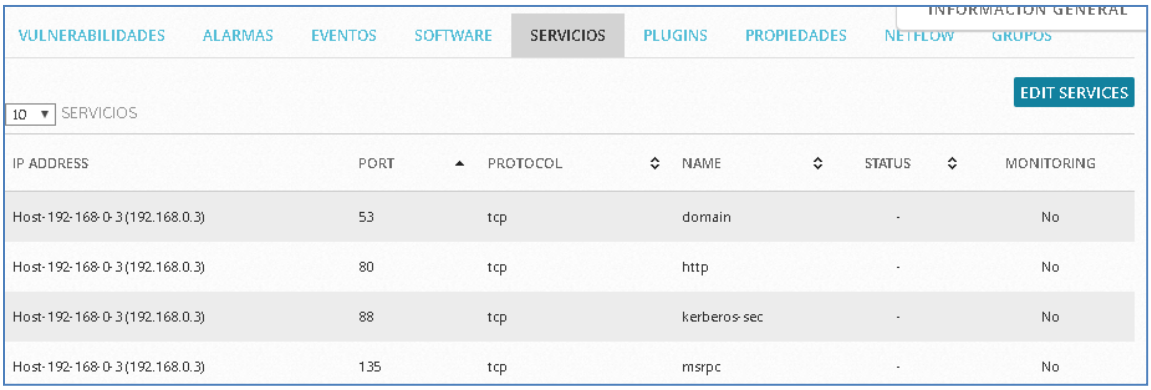


Figura No 208. Servicios del activo (Captura de pantalla de equipo personal)**.**

En el enlace "PROPIEDADES" mostrado en la **Figura No 209** podemos ver más información detallada del equipo. Como el numero MAC (Dirección física de la tarjeta de red del equipo).

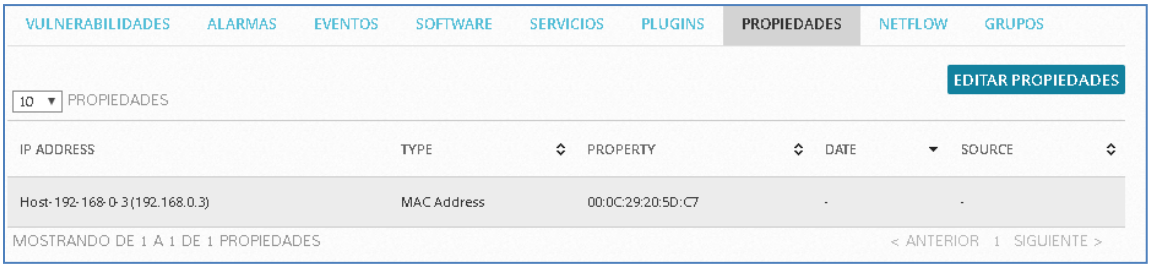


Figura No 209. Propiedades del activo (Captura de pantalla de equipo personal)

Si elegimos un tipo de informes como reporte de "Eventos SIEM". A continuación en la siguiente página se muestra en la **Figura No 210** parte de la portada del reporte que hemos recibido por correo.

Figura No 210. Portada informe eventos SIEM (Captura de pantalla de equipo personal)

La primera parte del reporte mostrado en la **Figura No 211** son los equipos que generan más ataques. Obsérvese que se incluye el mismo SIEM en el reporte puesto que cuando se realizan análisis de vulnerabilidades este ejecuta posibles exploit para probar si es susceptible o no un equipos.

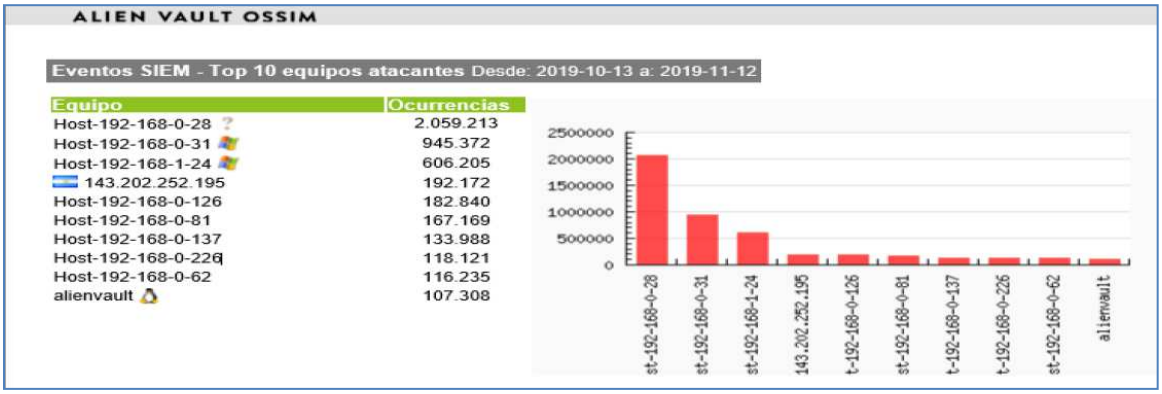


Figura No 211. Reporte de atacantes en eventos SIEM (Captura de pantalla de equipo personal)

Como se observa en la imagen de la **Figura No 212** se describen los puertos más utilizados en los eventos que el SIEM ha registrado. Con esto podemos saber que la mayoría de eventos los genera el servicio de internet (puerto 443) y por ende el DNS. Se detecta también que hay usuarios que utilizan el puerto

Telnet (TCP 23), SSH (TCP 22) y que el servicio de correos está utilizando también el puerto 465 (puerto TCP con seguridad SSL para correo.)

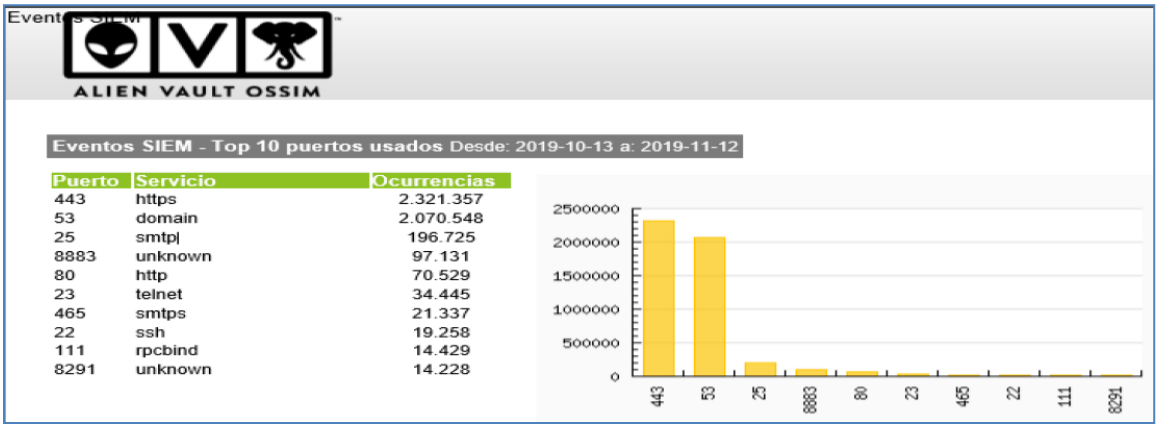


Figura No 212. Servicios detectados en reporte de eventos SIEM (Captura de pantalla de equipo personal)

Podemos también ver los equipos más atacados en la **Figura No 213**.

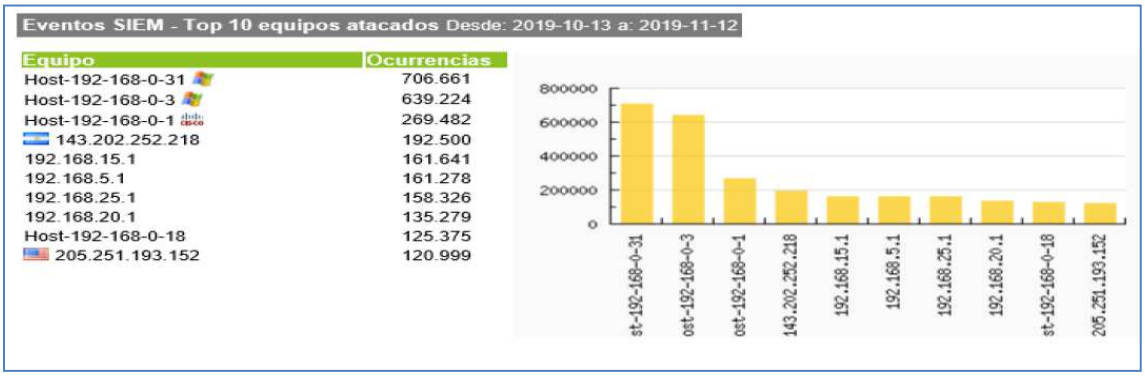
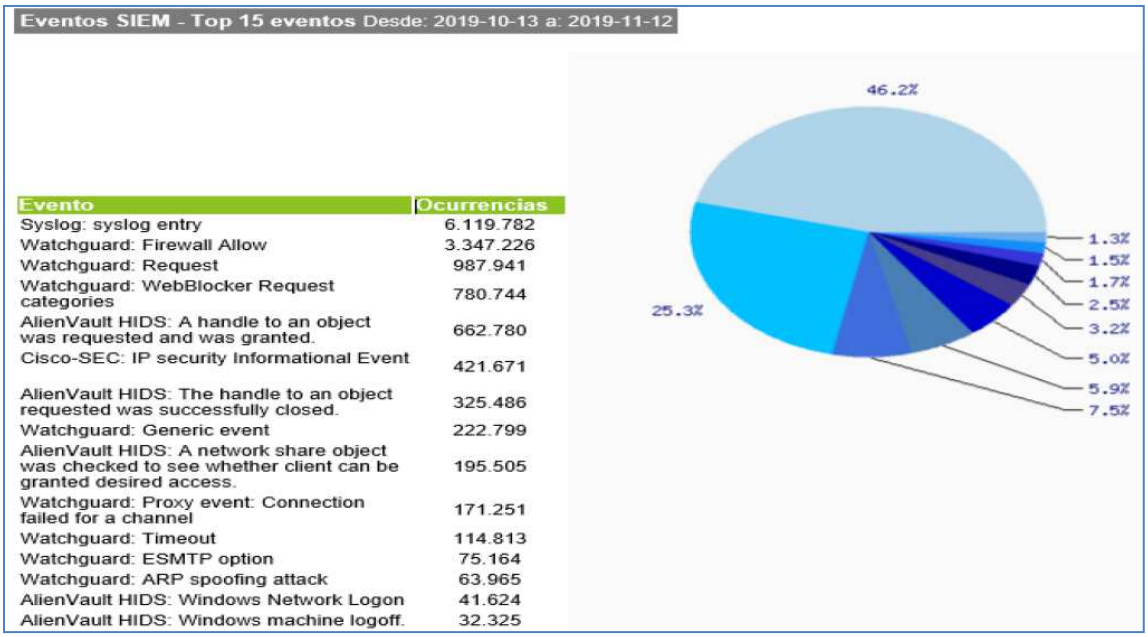


Figura No 213. Equipos atacados listados en reporte de eventos SIEM (Captura de pantalla de equipo personal)

En el mismo reporte generado se muestra en la **Figura No 214** los principales eventos registrados con sus ocurrencias. De esta tabla podemos observar que los mayores generadores de LOG son de un servidor Syslog, luego viene un seriado de eventos del Watchguard y se observan otros eventos de relevancias que nos permiten ver que está ocurriendo en el tráfico de la red.



Eventos SIEM - Top 15 eventos Desde: 2019-10-13 a: 2019-11-12

Evento	Ocurrencias
Syslog: syslog entry	6.119.782
Watchguard: Firewall Allow	3.347.226
Watchguard: Request	987.941
Watchguard: WebBlocker Request categories	780.744
AlienVault HIDS: A handle to an object was requested and was granted.	662.780
Cisco-SEC: IP security Informational Event	421.671
AlienVault HIDS: The handle to an object requested was successfully closed.	325.486
Watchguard: Generic event	222.799
AlienVault HIDS: A network share object was checked to see whether client can be granted desired access.	195.505
Watchguard: Proxy event: Connection failed for a channel	171.251
Watchguard: Timeout	114.813
Watchguard: ESMTP option	75.164
Watchguard: ARP spoofing attack	63.965
AlienVault HIDS: Windows Network Logon	41.624
AlienVault HIDS: Windows machine logoff.	32.325

Figura No 214. Reporte de eventos SIEM y sus ocurrencias (Captura de pantalla de equipo personal)

Los reportes de Eventos SIEM tiene la ventaja que ofrecen otros sub-reportes tales como: Eventos únicos SIEM, Sensores SIEM, Direcciones únicas de origen SIEM, Direcciones destino SIEM únicas y Puertos origen TCP/UDP SIEM entre otros.

10. CONCLUSIONES Y RECOMENDACIONES

10.1. CONCLUSIONES

Por medio de la implementación piloto llevada a cabo en la Empresa Administradora de Aeropuertos Internacionales se ha logrado observar y comprobar la importancia de poseer herramientas capaces de brindar una radiografía en tiempo real de lo que está pasando en la infraestructura tecnológica de la empresa. Más aun cuando todos somos susceptibles a cualquier intento externo por dañar la integridad, confidencialidad y disponibilidad de la información. Durante todo el tiempo de pruebas se obtuvieron datos impresionantes de la actividad de la red y los servicios que sustenta.

Durante todo el proceso de desarrollo del proyecto piloto de implementación de un sistema de monitoreo de eventos de seguridad basados en la implementación de un SIEM se pudo comparar que los tiempos de respuestas son inmediatos en la detección de anomalías y las trazas de auditoría que generan los equipos y todos los protocolos utilizados son fácilmente categorizados por el SIEM. Por medio del SIEM se pudo determinar que la mayoría del tráfico de la red es utilizado para servicio de internet y DNS.

Se ha dejado como recomendación el uso de un modelo general de monitoreo y gestión de eventos que se define en un diagrama de flujo de procesos. El modelo como tal pretende que la EAAI haga uso de la herramienta SIEM como el primer elemento de consulta en materia de cualquier problema o incidente de seguridad. A demás se propone que almacenen la información provista por el SIEM en una base de conocimientos. Con la utilización de este modelo y el software de gestión de servicios que la empresa está desarrollando tendrán los elementos suficientes para detectar anomalías o problemas, documentar, examinar y agilizar los tiempos de respuesta a los inconvenientes detectados por el SIEM.

Es de gran importancia para países como los nuestros hacer uso de herramientas de código abierto que permitan a los profesionales mejorar la funcionalidad de esos productos hasta llevarlos a niveles cercanos a las versiones de paga. Fomentar este tipo de herramientas contribuye al desarrollo profesional de todo individuo.

En materia de costos se logró comparar dos productos, el Splunk Enterprise y AlienVault USM/OSSIM, determinandose que aunque existen muchas fortalezas en el Splunk siendo además uno de los punteros en el cuadrante mágico de Garnert sus costos operativos y de mantenimiento de licencias son demasiado elevados e imposibilitarían a cualquier empresa debido a que son calculados en base a los LOG generados. En el caso del AlienVault USM que es la versión de paga del OSSIM es muy costosa para los niveles presupuestados por la EAAI en este tipo de gestión de seguridad; al igual que Splunk se base en LOG producidos por los dispositivos de red pero a menores costos. Por lo tanto la versión gratuita OSSIM es la que brinda posibilidad inmediata a la EAAI y a cualquier empresa de implementar mecanismos de seguridad que generan visibilidad completa de la infraestructura, generación de alarmas, detección de activos (escaneo de servicios, puertos, sistema operativo, software), escaneo de vulnerabilidades, detección de violaciones de seguridad o intrusiones, descubre comportamientos sospechosos brindando la posibilidad de analizar el trafico completo de la red y correlacionar todos los eventos de seguridad mostrando de forma inmediata cuadros de mandos que proveen en tiempo real la información del estado de la red.

En el caso de la EAAI en materia de costos no realizó inversión alguna para la implementación de este SIEM; a demás de ser gratuito y brindar muchas bondades. La EAAI posee equipos capaces de virtualizar sin problemas hasta dos SIEM en paralelo sin afectar los servicios activos permitiendo de forma inmediata la implementación del mismo. Cabe mencionar que no se debe pagar costos por mantenimientos anuales o soporte técnico ya que la empresa posee al personal calificado para realizar el mantenimiento, configuración y ajuste del SIEM instalado. Es importante mencionar que el OSSIM posee una suscripción gratuita a pulsos OTX que permiten intercambiar información crucial (Vulnerabilidades de día 0, Atacantes) entre todos los usuarios del OSSIM.

Durante todo el proceso de implementación, configuración, ajustes y pruebas se pudo constatar la efectividad de los dos SIEM elegidos en materia de detección de amenazas, anomalías o ataques. Ambos productos envían alertas y correos cuando se produce un evento de atente contra la seguridad. Más grande es la satisfacción saber que una versión gratuita tiene muy buen nivel de correlación, detección y análisis de la infraestructura de red. Si comparamos el modelo tradicional de gestión de LOG que es 100 % manual y que depende del ojo y razonamiento humano el OSSIM siempre será más efectivo. Los ataques efectuados de suplantación de IP, MAC y fuerza bruta para detección de contraseñas fueron perfectamente identificados por el SIEM.

El SIEM OSSIM tiene una característica integrada que le permite con el Netflow que escuchar el tráfico entre cualquier origen y destino permitiendo saber qué tipo de paquetes están viajando y que servicios se están implementando. Detectando en consecuencia patrones de tráfico de paquetes anómalos y permitiendo en su heurística una identificación temprana de tráfico dañino o fuera del parámetro real.

Durante un periodo de más de 6 meses se pudo probar dos SIEM. Se realizaron pruebas con SPLUNK observando que posee un poderoso motor de búsquedas y correlación. Pero que con el tiempo mientras más LOG se almacenan se decrementa el rendimiento del servidor y en temas de licencias como es por volumen de eventos sus costos en base a los cálculos del sitio Web son mayores que el AlienVault USM cotizado. En el caso del segundo producto que es AlienVault OSSIM (Código Abierto), similar al USM versión de paga, se encontró un proceso de configuración y administración bastante intuitivo. A demás este producto es gratis y brinda grandes funcionalidades de correlación, informes, análisis de eventos, cuadros de mandos, análisis de vulnerabilidades, gestión de activos y la posibilidad de modificar su código fuente para incluir otras funcionalidades. La única limitante de OSSIM es el manejo de los LOG en brutos que no puede ser accedido ya que es parte de la versión de paga

El desarrollo de la presente TESIS ha venido a contribuir en la EAAI ya que demostrado la importancia de poseer una visibilidad completa de lo que está pasando en la infraestructura de red. Con los equipos que se integraron al SIEM se ha observado que la mayor parte del tráfico de la red es INTERNET y DNS.

Instalar y configurar un SIEM es una tarea que requiere una base de conocimientos sólidos de toda la infraestructura de red y es de gran importancia que las empresas tengan bien configurados los equipos que generan la información al SIEM. Esto es vital ya que si el equipo fuente está mal configurado generará muchos falsos positivos en el SIEM.

El elemento a parte de la visibilidad que se ha comprobado que produce el SIEM es la ventaja de en tiempo real detectar cualquier comportamiento anómalo en la red o ataques. A demás la facilidad de detección de incidentes de seguridad y la reducción del tiempo en el análisis o interpretación de los LOG.

Mientras más equipos fuentes se integren al SIEM se permitirá al correlacionador de eventos tener un grado mayor de certidumbre en las clasificaciones de las alarmas y amenazas detectadas.

Con el SIEM no solo se tiene en un local todos los LOG centralizados para su posterior análisis sino también se posee un nivel de correlación de eventos que tendrían que utilizar más de 10 personas a la vez para ver los LOG de 5 equipos y aun así no lograrían tener la misma eficiencia, eficacia y velocidad que el motor de correlación y las alarmas. Esto se debe a que la velocidad a la que los eventos son generados por las distintas fuentes es muy grande para que los administradores de seguridad puedan ser eficientes. A demás el factor humano tiene variables incluidas que tienen que ver con cansancio, agilidad visual, conocimientos profundos de infraestructura de redes y servicios.

La herramienta SIEM de OSSIM no es un software aislado sino posee un marco de trabajo que incluye muchos otro software como NMAP, NESSUS, OSSEC, OpenVAS, Kismet, Nagios, OCS Inventory, NFsen, SNORT, Suricata, P0f y PADS. Esto le permite detección de intrusiones en clientes, escaneo de rootkits, neflow de la red, análisis de vulnerabilidades y de activos. Generando por tanto una solución que correlaciona todo un marco de trabajo capaz detectar, enlazar y aprender patrones de comportamiento en la red.

10.2. RECOMENDACIONES

Es necesario que todos los sensores manejen su hora y fecha sincronizadas. Para esto toda empresa debería tener implementado un servidor de hora (NTP, Network Time Protocolo - Protocolo de tiempo de red).

Es de gran importancia para la fiabilidad del SIEM que todos los sensores a integrar tengan una configuración adecuada y que hayan sido endurecidos para evitar que cualquier vulnerabilidad pueda ser explotada.

Es importante durante la etapa de análisis de requerimientos del SIEM poseer un diagrama completo de las infraestructuras de redes y servicios. Esto es importante ya que cuando se realiza el análisis de riesgos será mucho más fácil entender que recursos de la infraestructura de red son vitales para incluir en el SIEM. A demás esto garantizara que todas las fuentes que son integradas al SIEM no dejen de producir los LOG que son utilizados para las correlaciones y que generan mayor grado de certidumbre.

Desde el punto de vista de seguridad es importante que en las empresas se lleve a cabo una planificación de implementación de infraestructuras de seguridad basado en defensa por capas. Esto es muy bueno para el SIEM porque brinda mayores elementos que generen más certeza a los algoritmos y heurística que implementa el correlacionador de eventos.

Para un correcto uso de la herramienta SIEM se propone un modelo de gestión de eventos diagramado que se ubica en el **Anexo A-9** (Modelo de gestión de evento). Esto con el fin de aprovechar todo lo que brinda la herramienta y tener una base solida de conocimiento.

Para una implementación completa de todos los elementos de la infraestructura de red en base a los datos recabados de los dos SIEM implementados en este proyecto podemos definir un requisito de espacio en disco de al menos 1 TB por año.

11. GLOSARIO DE TÉRMINOS

WAN: Viene del acrónimo en inglés Wide Área Network en inglés o red de área amplia. Es una red de computadoras que une varias redes locales, aunque sus miembros no estén todos en una misma ubicación física.

UTM: Viene del acrónimo en inglés Unified threat management o Gestión unificada de amenazas, que comúnmente se abrevia como UTM, es un término de seguridad de la información que se refiere a una sola solución de seguridad y, por lo general, a un único producto de seguridad que ofrece varias funciones de protección en un solo punto en la red. Un producto UTM generalmente incluye funciones como antivirus, antispyware, antispam, firewall de red, prevención y detección de intrusiones, filtrado de contenido y prevención de fugas. Algunas unidades también ofrecen servicios como enrutamiento remoto, traducción de direcciones de red (NAT, network address translation) y compatibilidad para redes privadas virtuales (VPN, virtual private network).

LAN: Viene del inglés de Local Area Network o red de área local es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.

VPN: Responde a las siglas Virtual Private Network o red privada virtual, Es una red capaz de conectar varios dispositivos como si se encontrasen físicamente en el mismo lugar.

Hacker: Es una persona experta en el manejo de computadoras, que se ocupa de la seguridad de los sistemas y de desarrollar técnicas de mejora. Por lo general el término es empleado a las personas que ingresan de forma no autorizada a equipos de cómputo; pero esto es solo una de las definiciones según las clasificaciones existentes de los tipos de hackers.

FIREWALL: Conocido como cortafuego, es un dispositivo que hace las veces de vigilante informático, traza la línea divisoria entre el internet externo y un conjunto de máquinas de confianza.

IDS: Viene del acrónimo en inglés Intrusion Detection System o sistema de detección de intrusos. Consiste en un componente físico o software capaz de detectar ataques contra equipos de la red. Este utiliza una base de firmas o un conjunto de algoritmos para detectar anomalías en el tráfico de la red.

Intruso: Término empleado para referirse a cualquier persona o entidad que tiene intención maliciosa de obtener acceso no autorizado a recursos de la red.

IPS: Es parecido al IDS, viene del acrónimo en inglés Intrusion Prevention System o sistema de prevención de intrusos. Este dispositivo examina el tráfico de la red, determina si a dicha conexión se le concede el permiso de ingresar en virtud del contenido del paquete de datos.

Malware: Un tipo de software que tiene como objetivo infiltrarse o dañar un sistema de información sin el consentimiento de su propietario. Existen distintos tipos de malware en función de su origen y consecuencias. Entre ellos nos encontramos con los virus, gusanos, troyanos, keyloggers, botnets, spyware, adware, ransomware y sacareware.

Phishing: Este término es conocido como suplantación de identidad. Se utiliza para referirse a uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.

Logs: Registro oficial de eventos de distintas fuentes. Estas pueden ser de dispositivos de redes como switches, Routers o Equipos de computos como servidores de Aplicaciones, DNS, Dominio, Archivos.

Appliance: Aparato o Hardware con sistema operativo integrado. Pueden existir appliance de software.

Router: También conocido como ruteador o enrutador, este es un dispositivo de capa 3 (Capa de Red) encargado de determinar las mejores rutas o trayectorias de los paquetes de que recibe y envía.

Switch: En español denominado también Conmutador es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más host de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada ésta.

SIEM: (Security Information Event Management). Son dispositivos físicos o Software capaz de recibir, almacenar, procesar y relacionar registros logs de distintas fuentes

como IPS, IDS, Router, Switch, Servidores. Este tipo de herramienta es capaz de correlacionar eventos y establecer estrategias de identificación (Crea Reglas) y alertas.

SOC: Security Operation Center o Centro de Operaciones de Seguridad (COS). Es una central de seguridad informática que previene, monitorea y controla la seguridad en las redes y en Internet. Su función principal es proteger los equipos y redes de adversarios intelectuales que busquen violar la seguridad de la red.

NOC: Network Operation Center o Centro de Operaciones de Redes, es el área de la empresa encargada de monitorear, dar mantenimiento y solucionar los problemas en las redes de telecomunicaciones. Su función principal es mantener los equipos funcionando correctamente según los acuerdos de servicio y atender los incidentes que puedan afectar el desempeño de la red para mantener su disponibilidad al 100%.

Nagios: Software para monitoreo de dispositivos de red open source, es utilizado para monitorear dispositivos de red y servicios y proveer alertas en el evento de indisponibilidad.

OCS Inventory: Brinda la capacidad de administración de activos multiplataforma, esta herramienta provee una forma automatizada de mantener un registro del software que se tiene instalado en los hosts

NFSen: Es un Netflow, poderoso artefacto para análisis de tráfico de red y es muy valorado en el proceso de correlación, provee una interfaz gráfica web donde se presentar graficas del tráfico en la red.

Ntop: Herramienta de trafico de red, brinda3 información invaluable acerca de tráfico en la red, la cual puede ser utilizada para detectar trafico anormal o malicioso de forma proactiva.

Snort: Es un IDS código abierto muy importante, una versión personalizada está integrado dentro de OSSIM y provee alertas relacionadas con ataques en la red.

Suricata: Es un IDS alternativo a Snort, el cual es compatible totalmente con las reglas de snort. A diferencia de snort es multi-hilo.

P0f: Es una herramienta utilizada para escaneo pasivo de sistema operativo (descubrimiento del tipo de sistema operativo y versión)

PADS: Sistema de detección de activos pasivo, es una herramienta que monitorea silenciosamente tráfico de red y registra actividad de hosts y servicios en la red, estos datos pueden ser monitoreados por OSSIM para analizar anomalías en la red.

Nmap: Herramienta utilizada para descubrimiento de host y enumeración de puertos abiertos en los hosts de la red, así como para descubrir sistemas operativos y versiones de los hosts.

OpenVAS: Es la versión con licencia GPL de Nessus, se utiliza para realizar escaneo de vulnerabilidades de activos en la red, esta información es almacena en la base de datos de OSSIM.

OSSEC: Es un sistema de detección de intrusos basado en host (HIDS), esta herramienta provee análisis de logs multiplataforma, chequeo de integridad de archivos, detección de rootkit, monitoreo de políticas y monitoreo de alerta y respuestas en tiempo real, esta herramienta ayuda a proteger a OSSIM a sí mismo.

Kismet: Es una herramienta para detección de intrusos en redes inalámbricas (WIDS), funciona para detectar falsos AP

12. REFERENCIAS BIBLIOGRÁFICAS

[01] *AT&T CyberSecurity.* (20 de 05 de 2019). Obtenido de Alienvault: https://www.alienvault.com/documentation/usm-appliance/events/event-details-fields.htm

[02] Chicano Tejada, E. (2014). *Gestión de Incidentes de Seguridad Informática* (1ª Edición ed.). (I. Editorial, Ed.) Andalucía, España: © IC Editorial, 2014.

[03] David Miller, S. H. (2010). *Security Information and Event Management (SIEM) Implementation.* New York: McGraw-Hill Education.

[04] *firma-e.com*. (14 de 10 de 2014). Obtenido de firma-e.com : https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/

[05] *https://es.wikipedia.org (log)*. (05 de 09 de 2018). Obtenido de https://es.wikipedia.org: https://es.wikipedia.org/wiki/Log_(informática)

[06] *iso27000.es*. (04 de 09 de 2018). Obtenido de ISO 27001: http://www.iso27000.es/download/doc_sgsi_all.pdf

[07] Kelly Kavanagh, T. B. (26 de 02 de 2018). *Magic Quadrant for Security Information and Event Management*. Obtenido de www.gartner.com: https://www.gartner.com/doc/reprints?id=1-4LC8PAW&ct=171130&st=sb

[08] *Repositorio Institucional UPV (Universidad Politecnica de Valencia)*. (10 de 12 de 2008). Obtenido de riunet.upv.es: https://riunet.upv.es/bitstream/handle/10251/13179/Tesina.pdf?sequence=1

[09] Secur-IT @C.R.S. (05 de 09 de 2018). *securitcrs.wordpress.com*. Obtenido de Secur-IT @C.R.S.: https://securitcrs.wordpress.com/knowledge-base/siem-security-information-and-event-management/

[10] SOFISTIC. (05 de 09 de 2018). *SOFISTIC (SIEM)*. Obtenido de sofistic.com: https://www.sofistic.com/productos/security-information-and-event-management-siem/

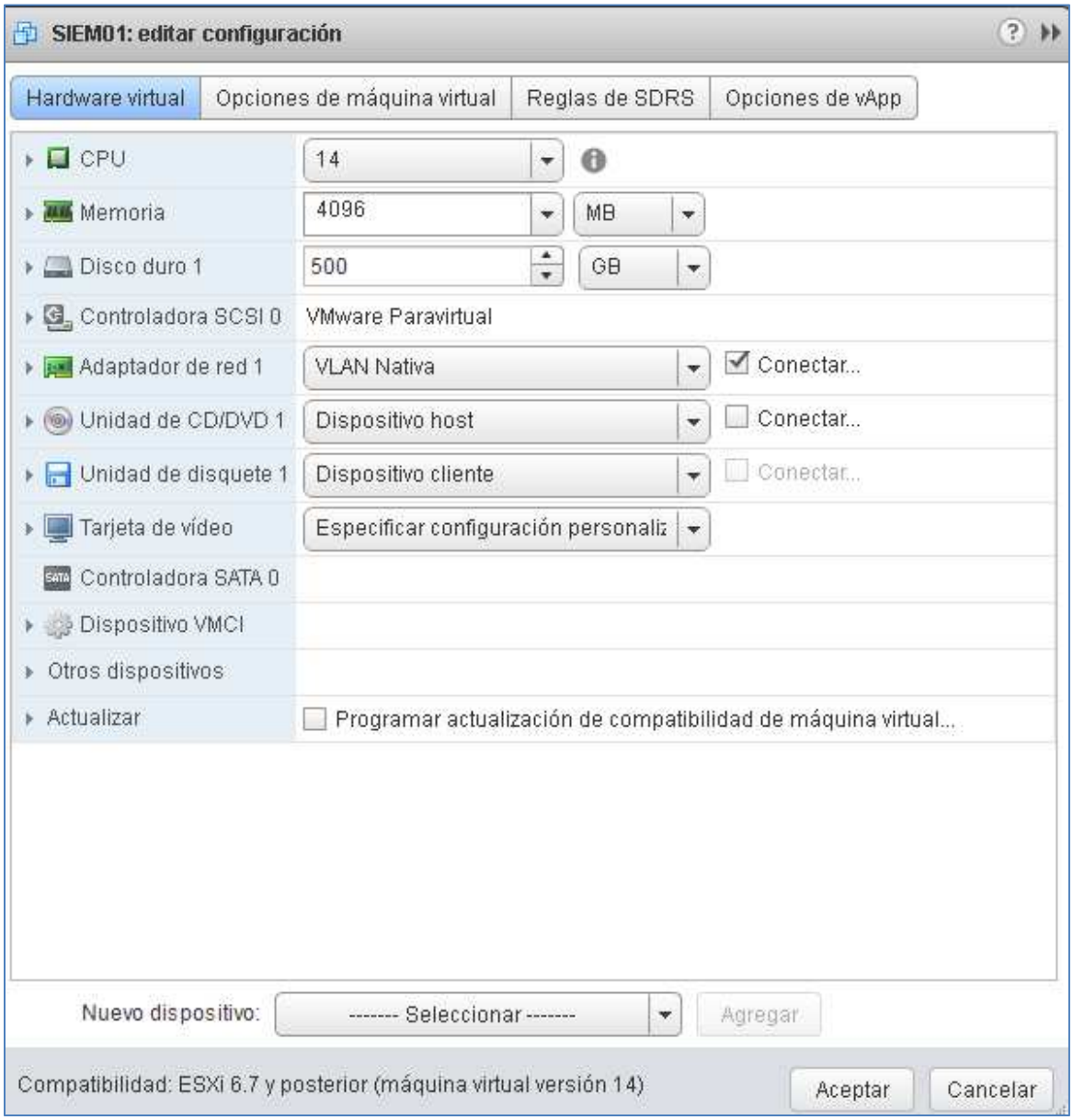
[11] Sweeny, J. (20 de Junio de 2011). *SANS Institute Reading Room site*. Obtenido de www.sans.org: https://www.sans.org/reading-room/whitepapers/incident/creating-siem-incident-response-toolkit-open-source-tools-33689

[12] *Wikipedia.org (Seguridad de la Información)*. (04 de 09 de 2018). Obtenido de Wikipedia: https://es.wikipedia.org/wiki/Seguridad_de_la_información

13. ANEXOS

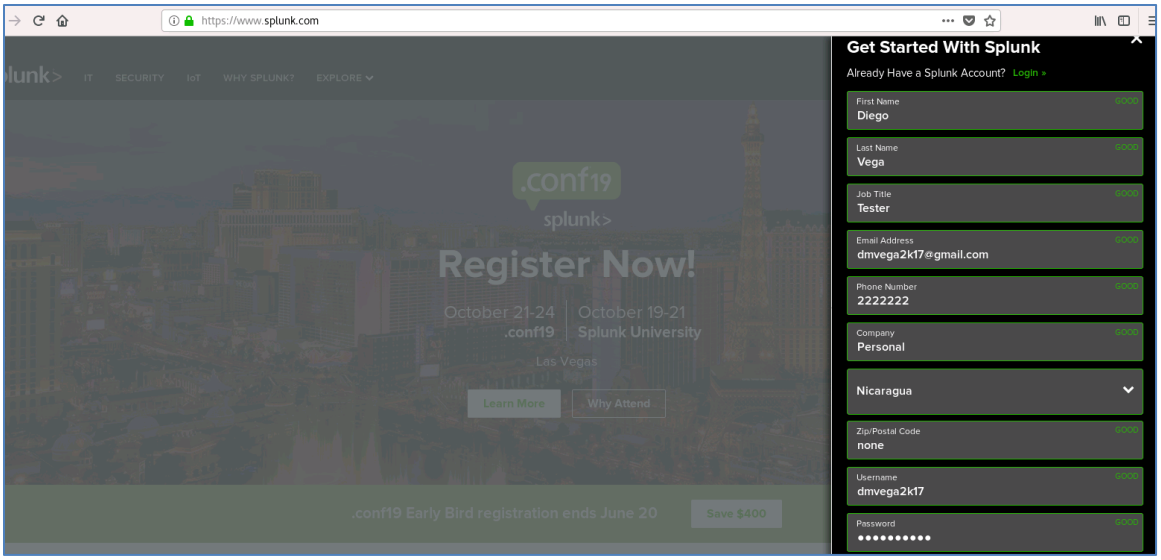
A-1. Proceso de Instalación de Splunk

Para llevar a cabo la instalación del software Splunk se ha decido utilizar como plataforma el sistema operativo Centos 7. El hardware que se utiliza es de un equipo virtual. La configuración de la máquina virtual para splunk es la siguiente:

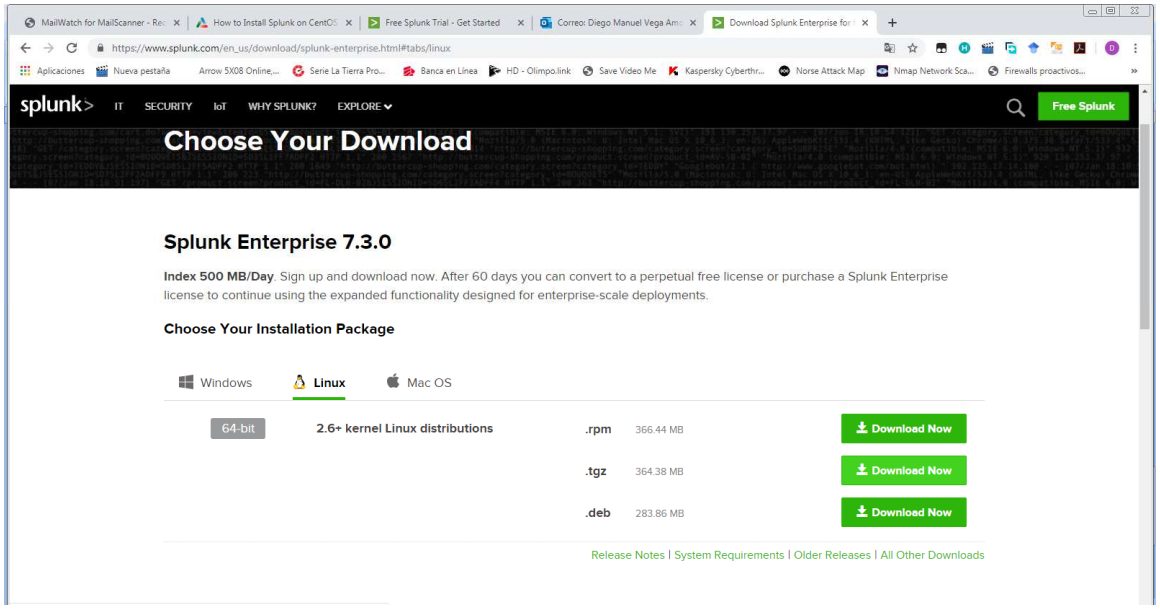


Una vez terminado el proceso de instalación de Centos 7 se procede a configurar en el mismo una carpeta compartida llamada público donde se

copiara el archivo comprimido del Splunk. En el sitio web de Splunk se procede a efectuar el registro de una nueva cuenta para poder descargar el software.

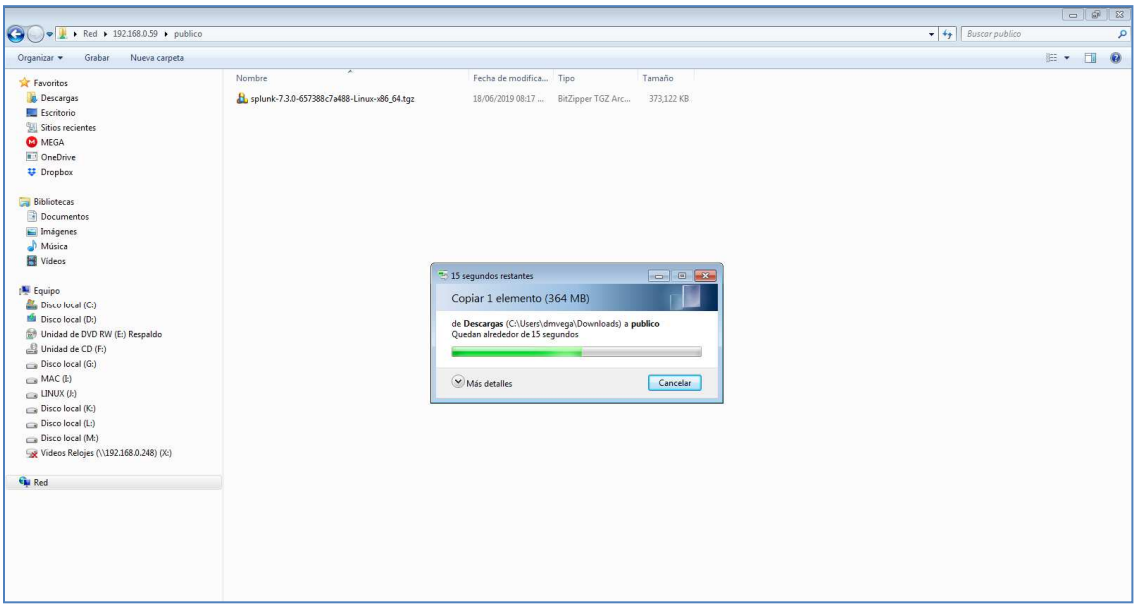


Una vez registrado el usuario el sitio nos redirecciona a elegir el software de nuestra conveniencia.

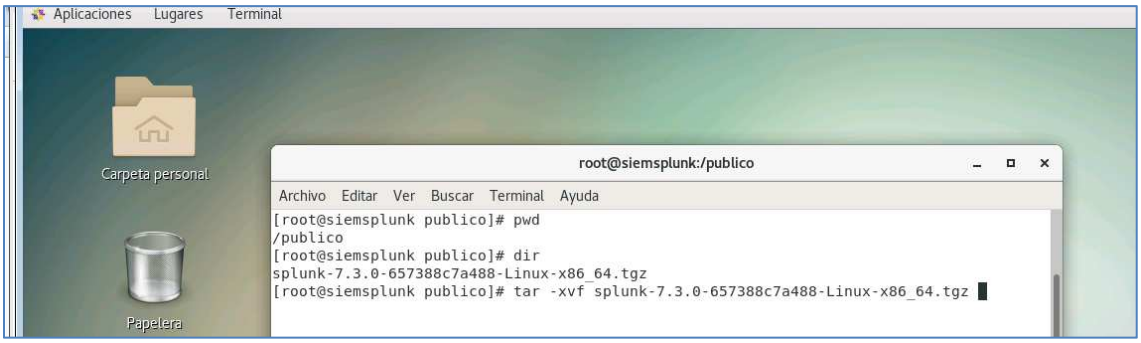


En este caso descargamos la versión para Linux del tipo tgz. Una vez descargada lo que sigue es el traslado del software el servidor Centos 7.

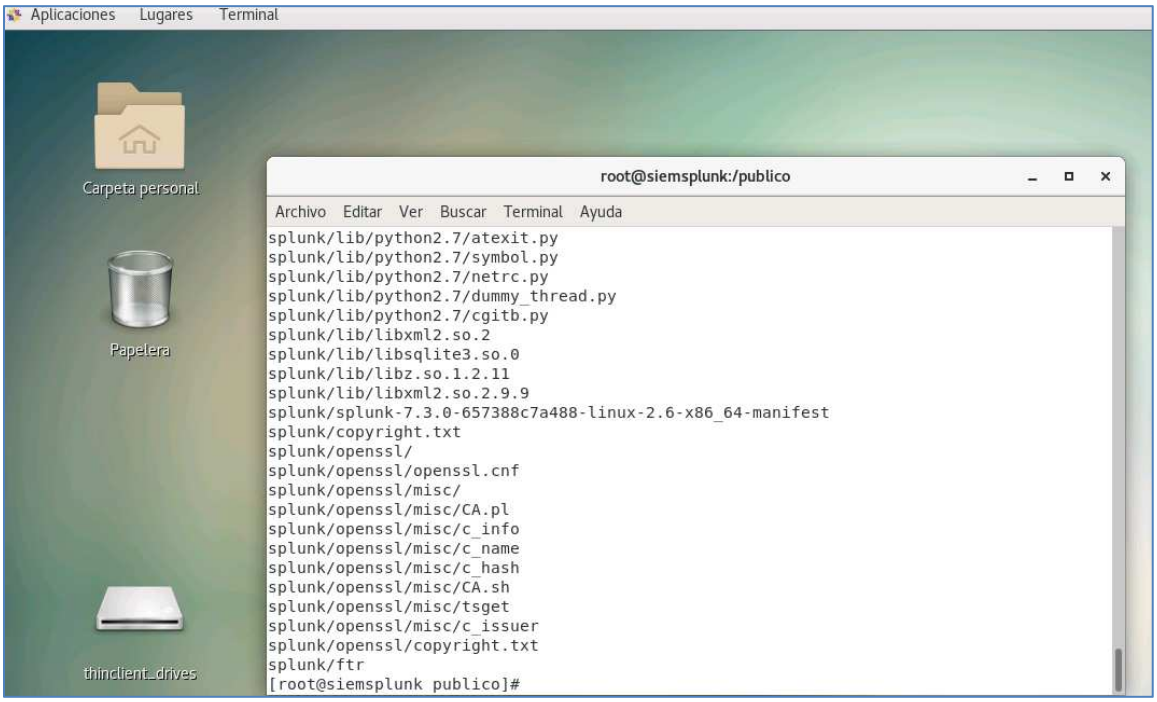
En esta imagen se observa la copia al directorio compartido de Centos.



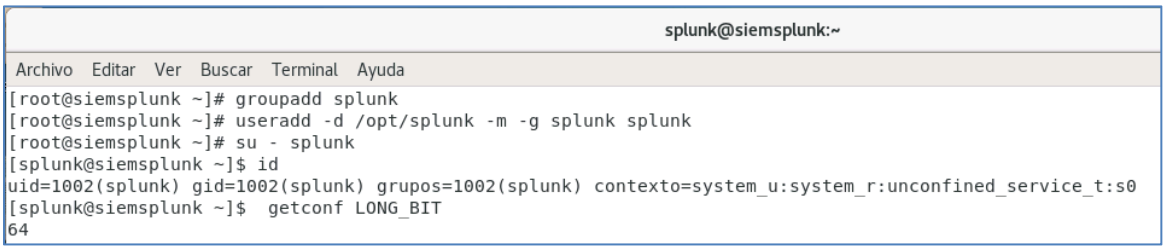
Lo siguiente es descomprimir el archivo descargado



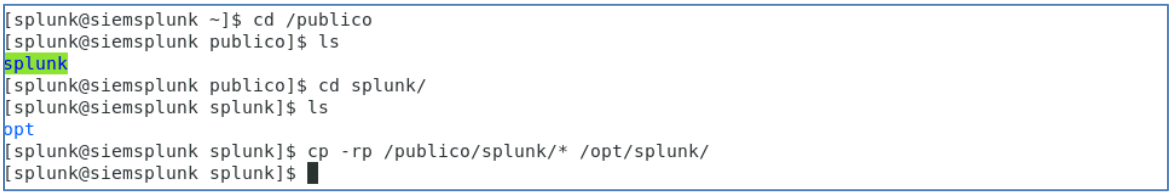
Se puede observar que el archivo ha sido descomprimido sin problemas.



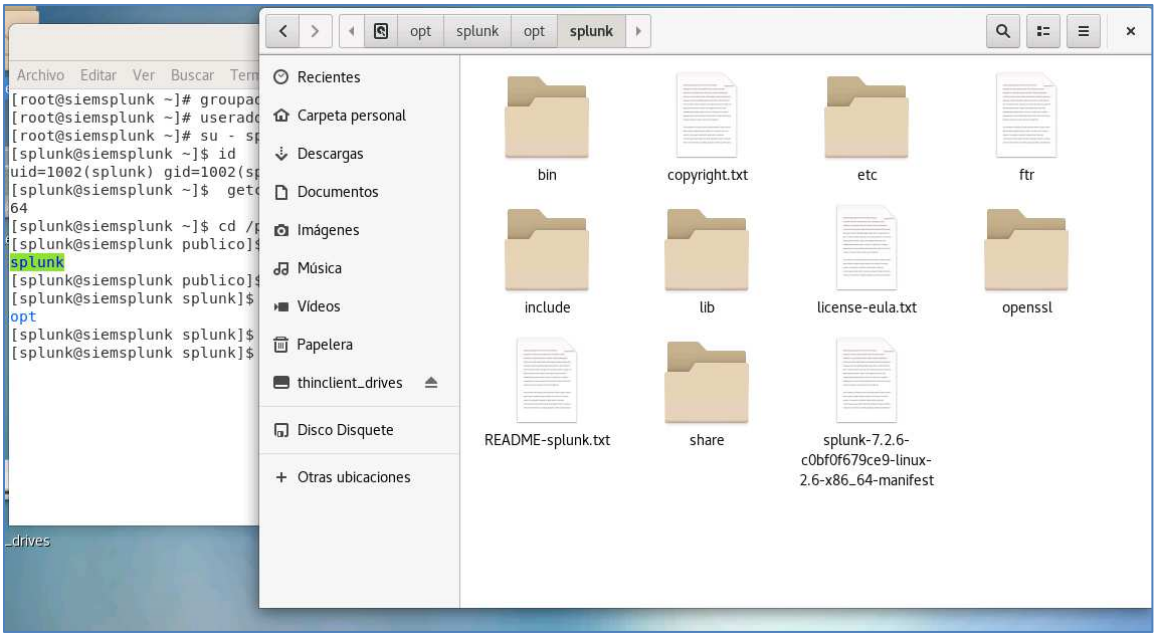
Antes de instalar se debe crear un grupo y usuario llamado **splunk**. A este usuario se le asigna como directorio principal **/opt/splunk** que fue creado con anticipación. Tal como se muestra en la siguiente imagen.



Con el usuario ya logado procedemos a ir al directorio donde se descomprimió Splunk y procedemos a copiarlo en la ruta /opt/splunk. Tal como se oberva en la imagen de abajo.



Como se puede observar en la imagen que sigue los archivos han sido copiados con éxito.

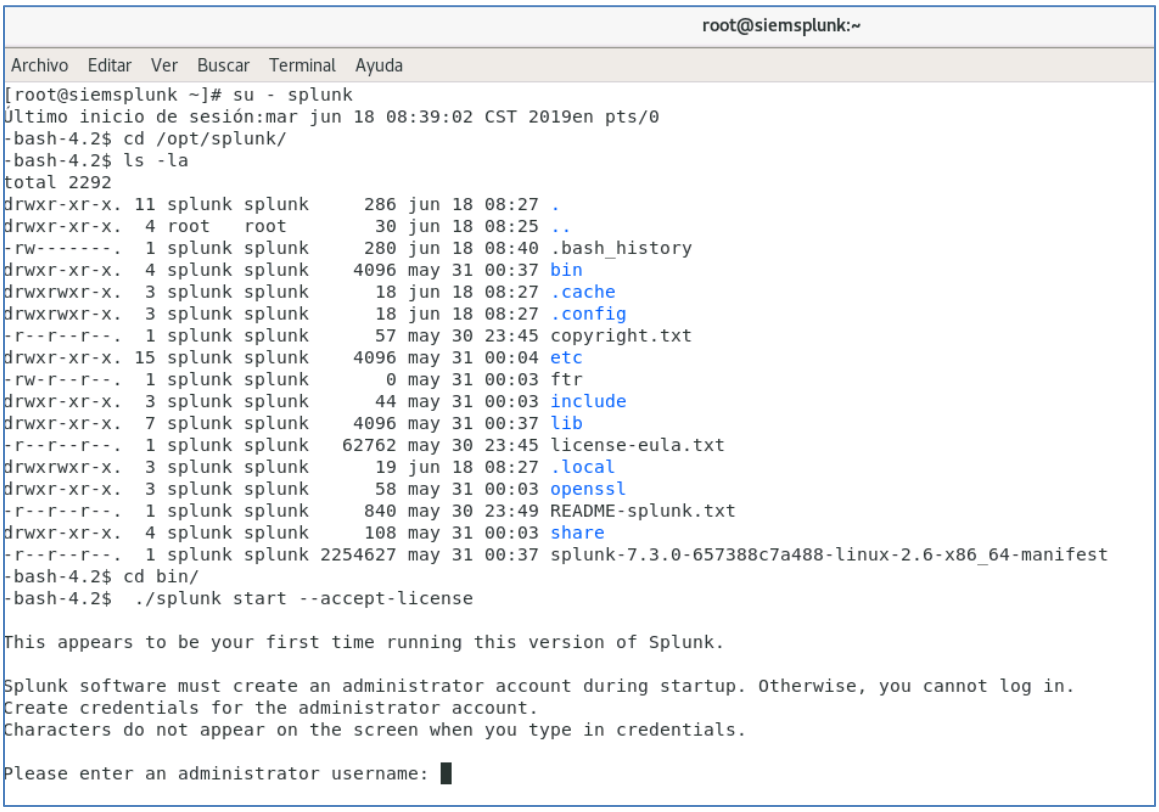


Una vez copiado los archivos es necesario reconfigurar los permisos y establecer como grupo y usuario dueño de los archivos a: splunk

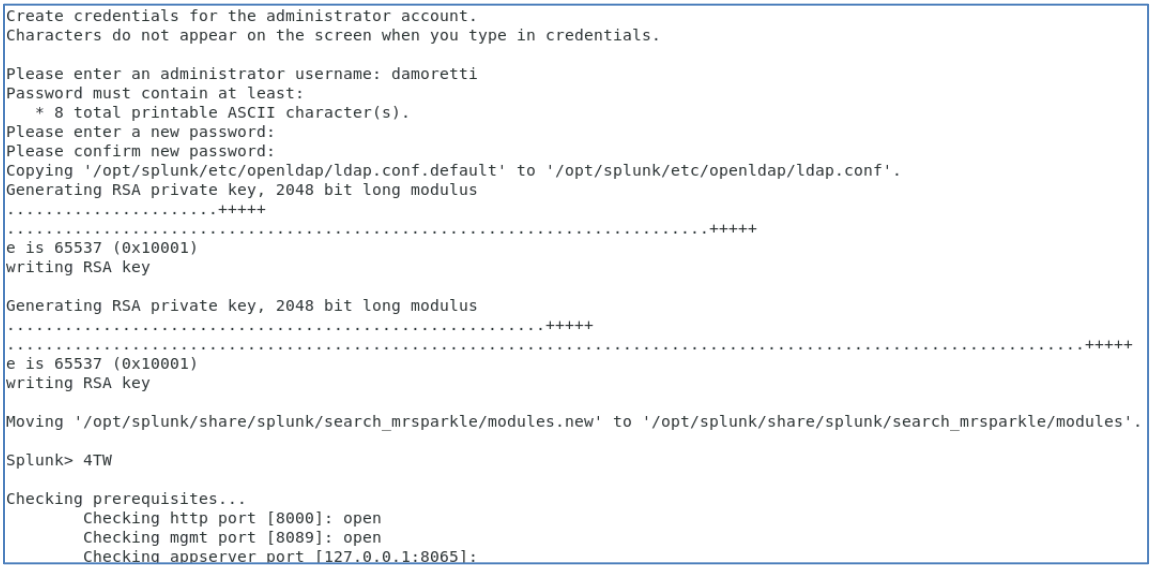
```
[splunk@siemsplunk splunk]$ cp -rp /publico/splunk/* /opt/splunk/
[splunk@siemsplunk splunk]$ chown -R splunk: /opt/splunk/
[splunk@siemsplunk splunk]$ cd /opt/splunk/opt/splunk/
[splunk@siemsplunk splunk]$ ls -la
total 2432
drwxr-xr-x.  8 splunk splunk     222 jun 17 16:16 .
drwxr-xr-x.  3 splunk splunk      20 jun 17 16:13 ..
drwxr-xr-x.  4 splunk splunk    4096 jun 17 16:14 bin
-rwxr--r--.  1 splunk splunk      57 abr 11 06:52 copyright.txt
drwxr-xr-x. 15 splunk splunk    4096 jun 17 16:14 etc
-rwxr--r--.  1 splunk splunk       0 abr 11 07:05 ftr
drwxr-xr-x.  3 splunk splunk      44 jun 17 16:15 include
drwxr-xr-x.  7 splunk splunk    4096 jun 17 16:16 lib
-rwxr--r--.  1 splunk splunk   63714 abr 11 06:52 license-eula.txt
drwxr-xr-x.  3 splunk splunk      58 jun 17 16:16 openssl
-rwxr--r--.  1 splunk splunk     842 abr 11 06:55 README-splunk.txt
drwxr-xr-x.  3 splunk splunk      86 jun 17 16:16 share
-rwxr--r--.  1 splunk splunk 2404340 abr 11 07:37 splunk-7.2.6-c0bf0f679ce9-linux-2.6-x86_64-manifest
```

En esta etapa ya se está listo para dar inicio a la instalación de Splunk.

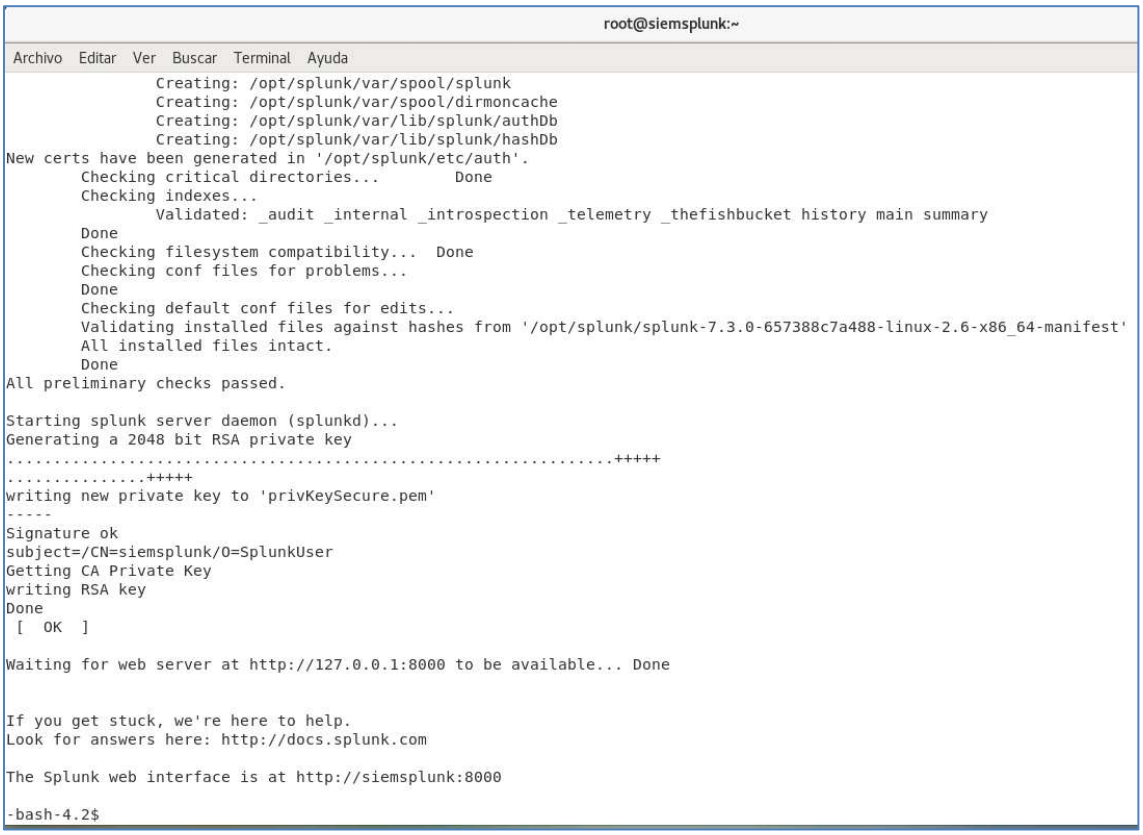
En este momento hacemos logueo con el usuario splunk y ejecutamos el comando: **./splunk start –accept-license** desde el directorio **bin**. Tal como se observa en la siguiente imagen.



Lo que resta en este momento es ingresar el nombre de usuario y la clave del que será administrador del Slunk tal como se muestra en la siguiente imagen.

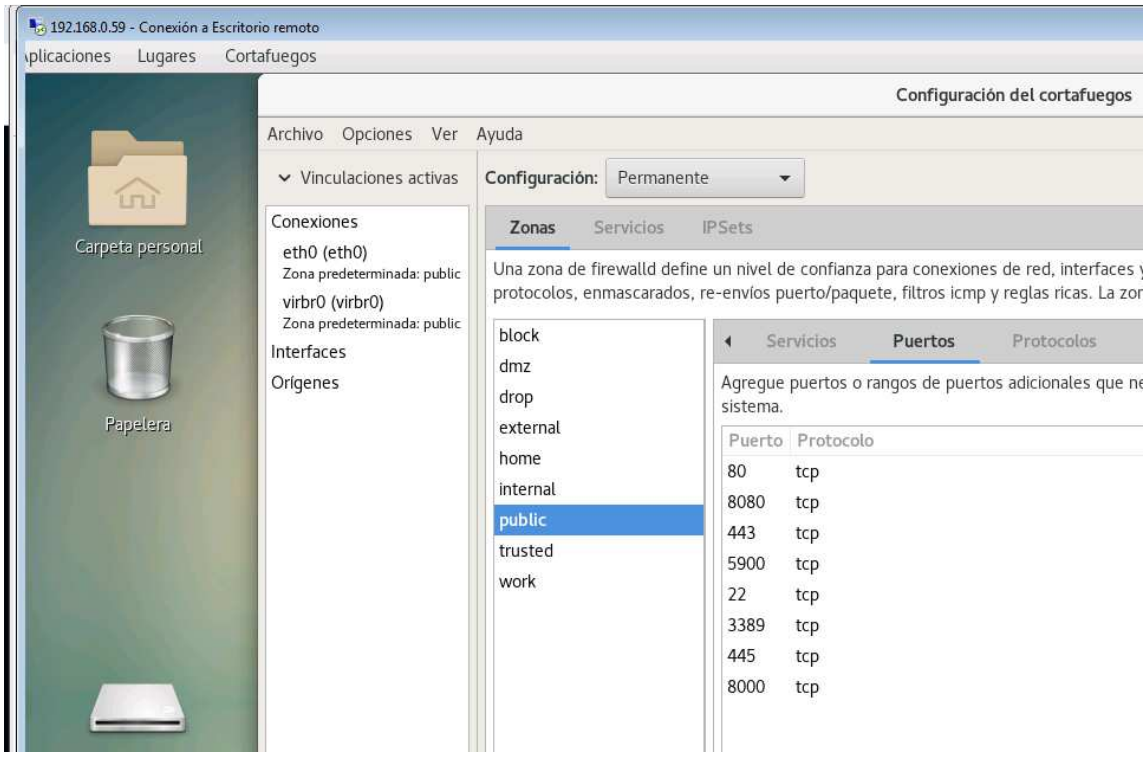


Con la clave ya ingresada el instalador continua su proceso y genera una clave de seguridad que es un certificado RSA de 2048 bit. Esto es para seguridad en sus conexiones.



Una vez el Splunk ya instalado queda disponible para su gestión desde el IP 192.168.0.59 que es del servidor Splunk en el puerto 8000.

Lo siguiente tarea a realizar es agregar en el firewall la regla que permita el acceso al puerto 8000 desde cualquier equipo de la LAN. La Figura de la página siguiente muestra dicha configuración de forma gráfica.



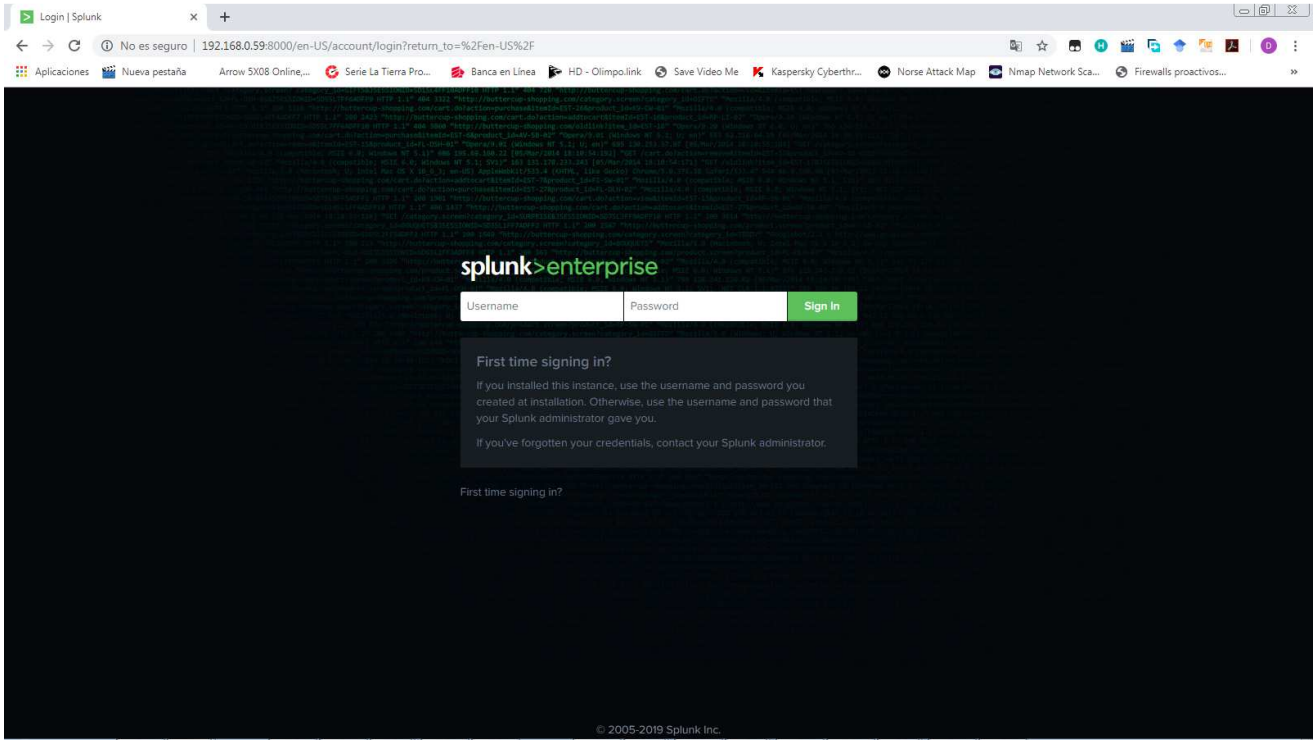
Como se observa en la figura de arriba se ha configurado en la zona pública los puertos requeridos a estar visibles en el exterior. Dentro de esos puertos está el puerto de gestión del Splunk, que es el TCP 8000. Con la configuración del firewall realizada podemos acceder sin problemas al Splunk Enterprise.

Es importante en esta etapa tener en cuenta que aunque el Splunk Enterprise está perfectamente instalado pero si no se configura la opción vía comando para que se inicie cada vez que el equipo se apague o reinicie no levantará de forma automática. Por tanto se ejecuta el siguiente comando:

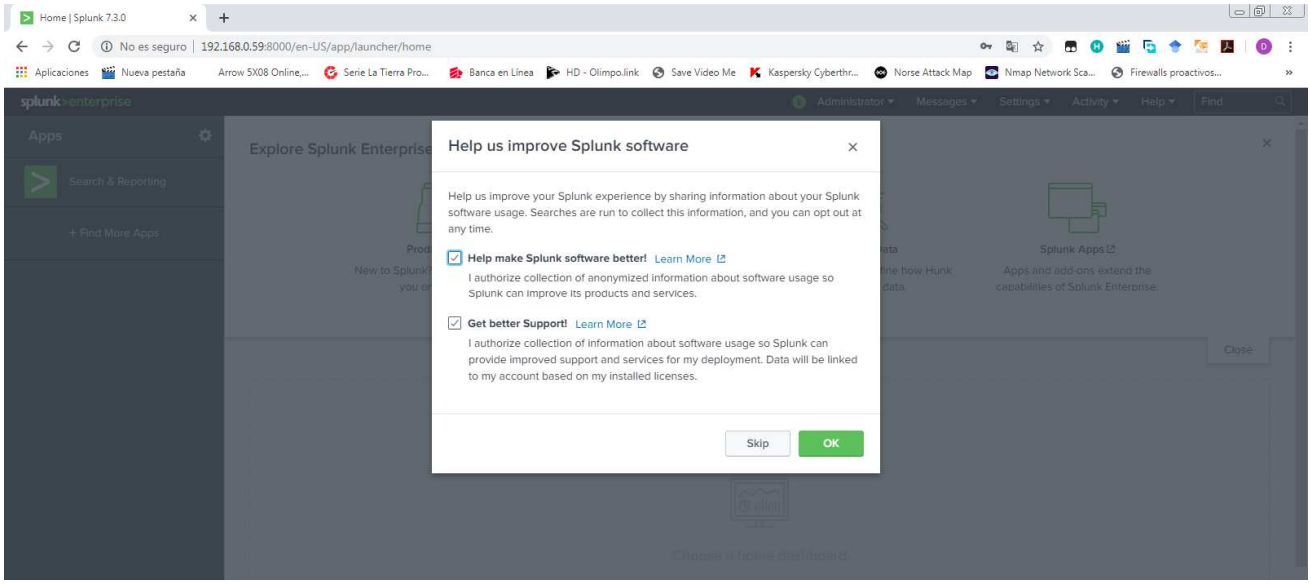
```
/opt/splunk/bin/splunk enable boot-start
```

De esta forma aseguramos que el Splunk Enterprise este siempre disponible.

Lo que muestra la imagen que sigue es la interfaz web de gestión del Splunk.

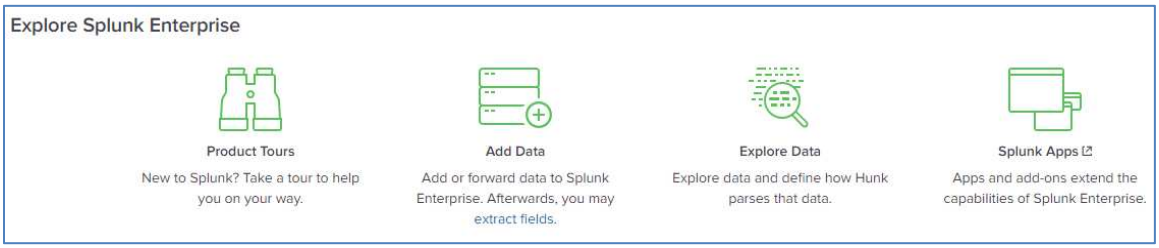


Ingresamos con el usuario damoretti y la clave de acceso. Nos muestra en la imagen de abajo una pantalla de bienvenida. Ahora lo que resta es configurar sensores, reglas, alertas y realizar búsquedas en la base de datos de eventos.

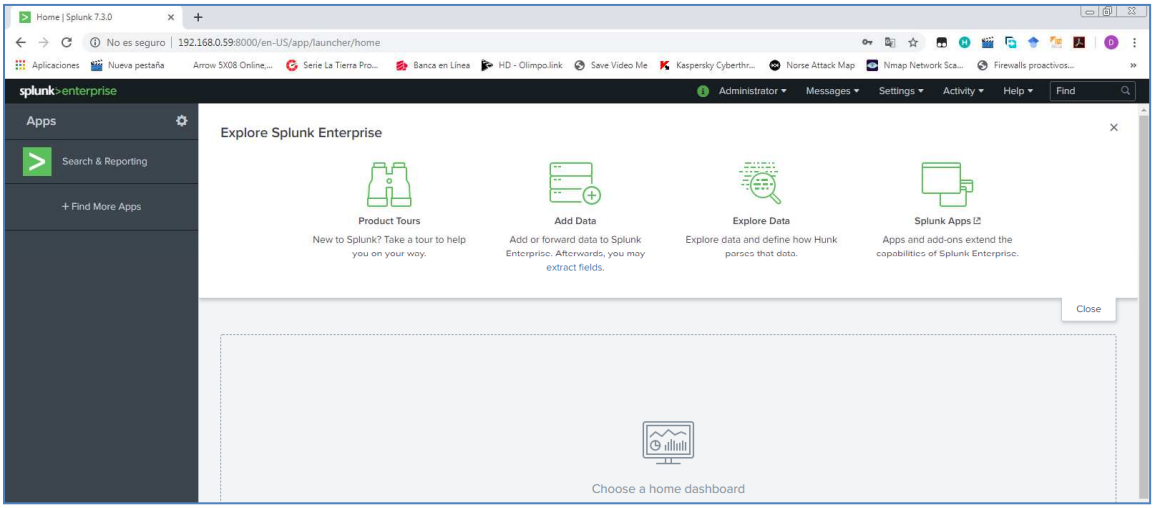


A-2. Integración de equipos al Splunk Enterprise.

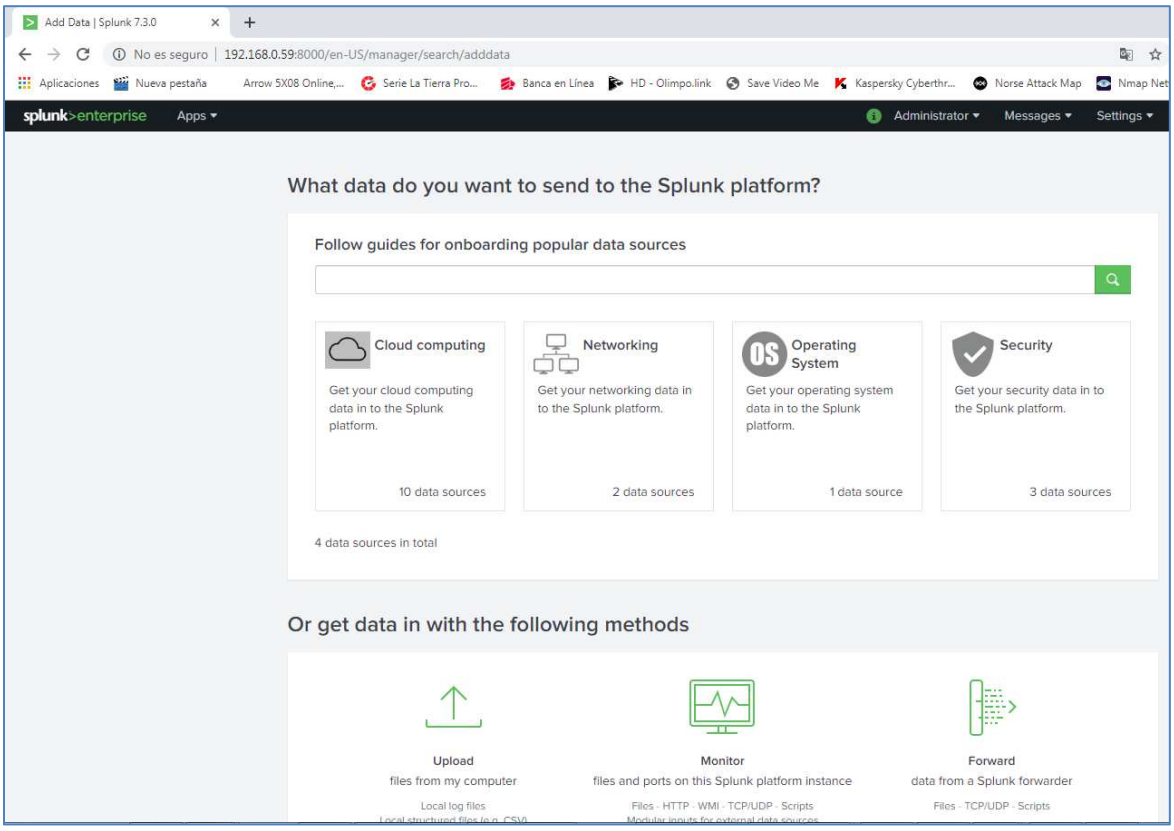
En el menú principal el Splunk posee cuatro opciones. La primera opción Product Tours, es un simple pasee por el producto indicando que son los componentes y la forma en que se debe iniciar a configurar los orígenes de datos de los LOG. La segunda opción Add Data permite mostrar en forma general todas las posibles fuentes de integración de datos que Splunk admite. La tercera opción Explore Data es utilizada para realizar análisis de los datos almacenados en el sistema. La cuarta y última opción es Splunk Apps, esta opción permite al usuario descargar todas las Apps disponibles en línea para administrar la data de splunk. Estas Apps contienen diferentes tipos de analítica y cuadros de mando que pueden ser personalizados por los usuarios. Tal como se muestra en la imagen que sigue.



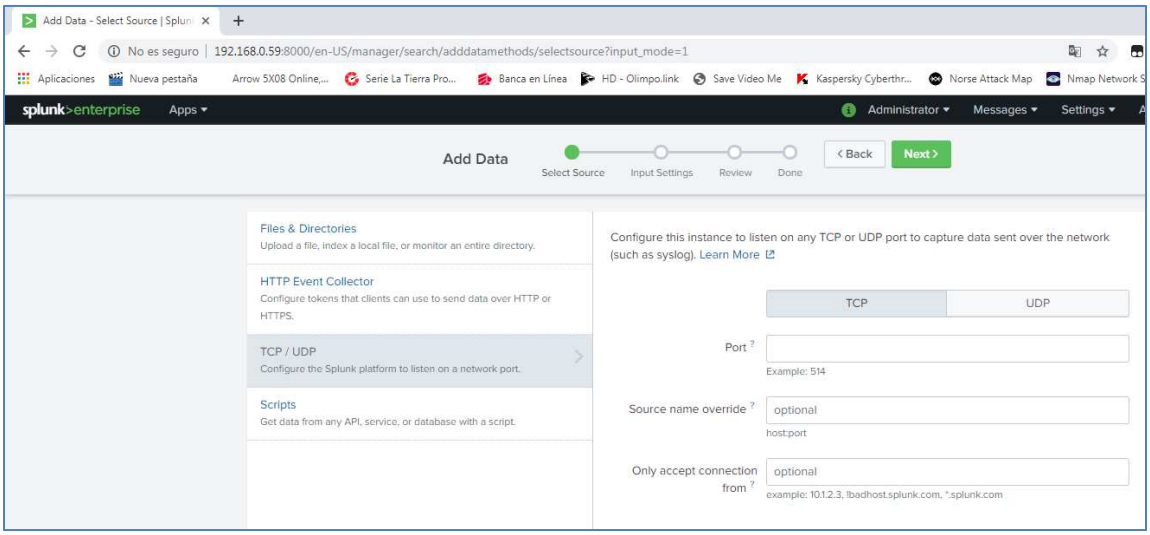
Lo siguiente es la pantalla completa que aparece una vez que cerramos la pantalla de bienvenida.



Seleccionamos la opción **Add Data** para conocer los distintos tipos de métodos de obtención de datos que admite splunk. Tal como se muestra en la imagen que sigue.



Seleccionamos la opción Monitor para agregar un dispositivo de la red. En la opción Monitor se presentan cuatro distintas opciones de recolección de datos. La primera es para archivos y directorios (**Files & Directories**), la segunda es por medio de http (**Http Event Collector**), la tercera es para especificar puertos de escucha (**TCP/UDP**) como el syslog o cualquier otro que permite captura de datos y la última opción es para capturar por medio de programas (**Scripts**). En nuestro caso seleccionamos TCP/UDP para agregar una fuente de datos tipo syslog. Tal como se muestra en la imagen de inicio de la siguiente página.



El único inconveniente que se enfrenta en esta etapa es que por defecto el Centos 7 trae instalado un rsyslog que a su vez utiliza por detecto el puerto UDP 514. A demás de lo mencionado el sistema operativo no permite que usuarios no root (como el splunk que creamos) hagan uso de puertos menores al 1024, como es el caso de syslog. Por tanto hay que realizar cambios. Se debe ejecutar por medio de una terminal una regla de preruteo que indique al equipo que al recibir información por el puerto UDP 514 lo envíe al puerto udp 5447

/usr/sbin/iptables -t nat -A PREROUTING -m udp -p udp --dport 514 -j REDIRECT --to-ports 5447

Ahora si estamos listos para integrar nuestro primer equipo. En este caso utilizaremos el Router Cisco de Backup para probar la carga de datos del Router principal por medio de un espejo de puertos en el Switch core. En el Router Cisco se debe configurar el envío de LOG a un equipo remoto. Para este efecto se deben ejecutar los siguientes comandos en el router.

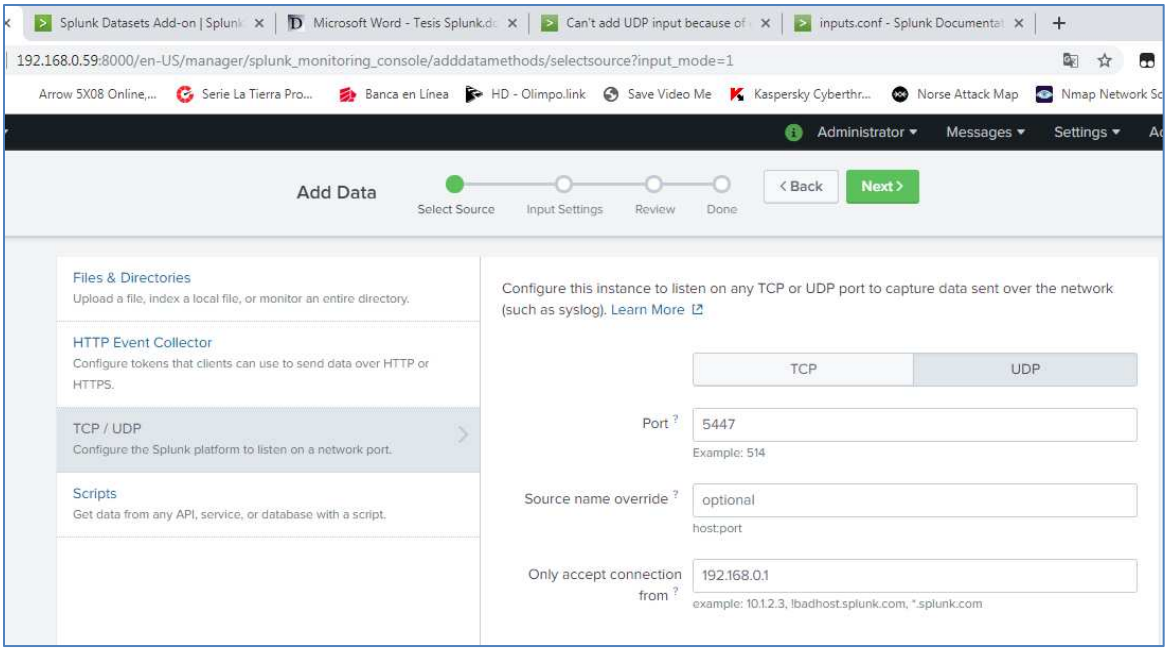
service timestamps log datetime msec localtime show-timezone year
logging userinfo
logging buffered 21474836 errors
logging rate-limit 10000
logging trap debugging

logging server-arp

logging host 192.168.0.59

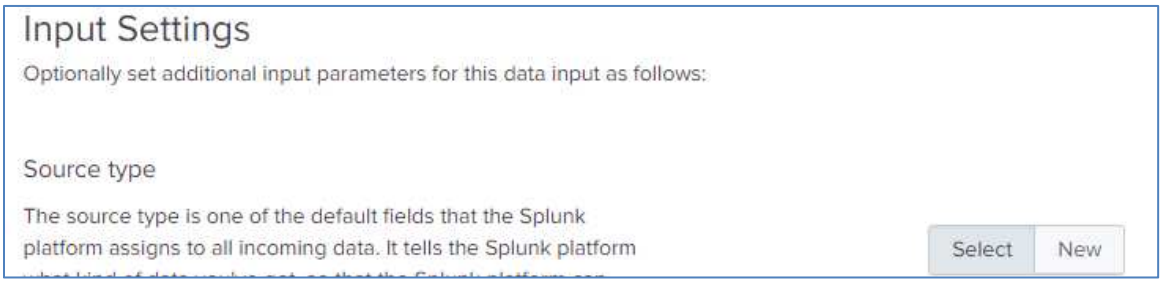
logging trap

En la imagen que sigue podemos observar el inicio de la configuración de un sensor por medio de syslog y el puerto que utilizamos es el UDP 5447, que fue el que configuramos en la política de re-direccionamiento por el problema mencionado.

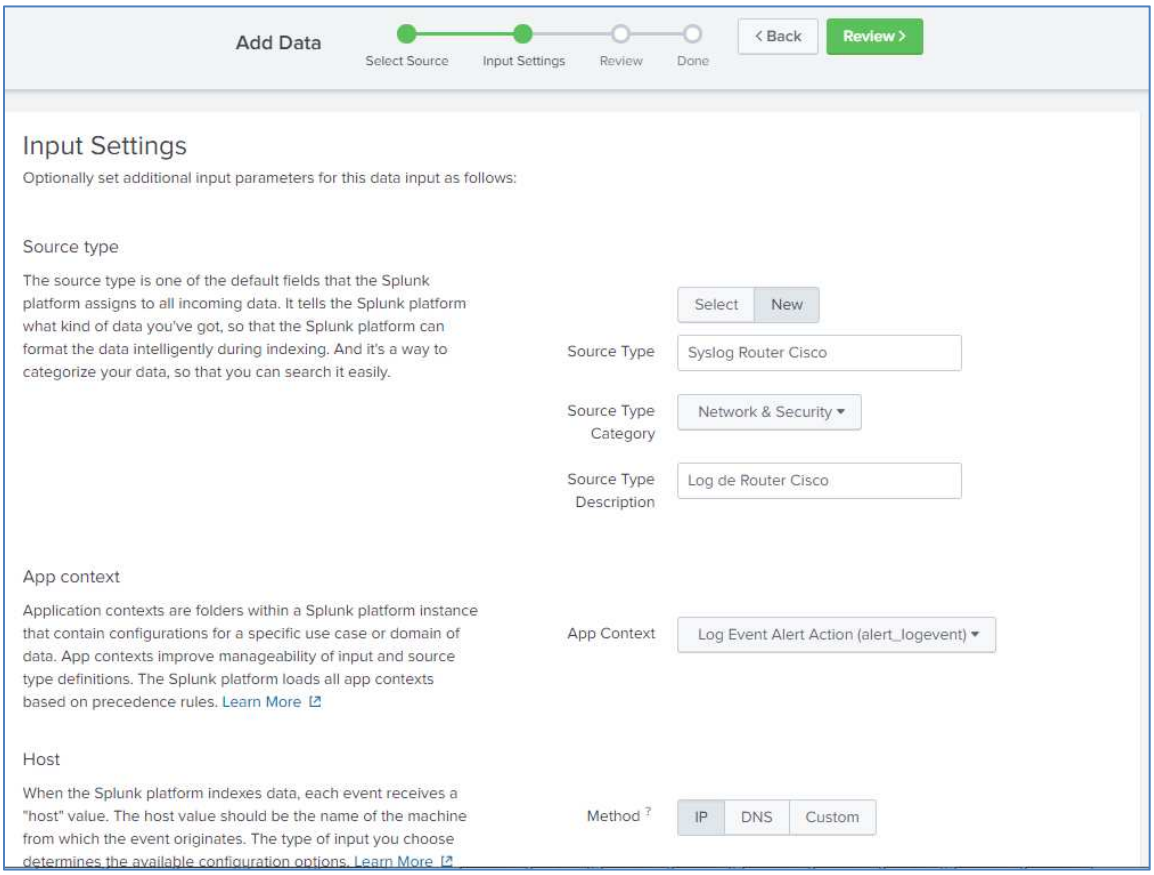


En esta etapa solo se ingresa en el campo Port el puerto equivalente a lo interno del servidor al UDP 514, que es el UDP 5447 que fue creado en la regla de preruteo y en el campo Only accept connection se ingresa el IP del equipo que deseamos obtener los LOG.

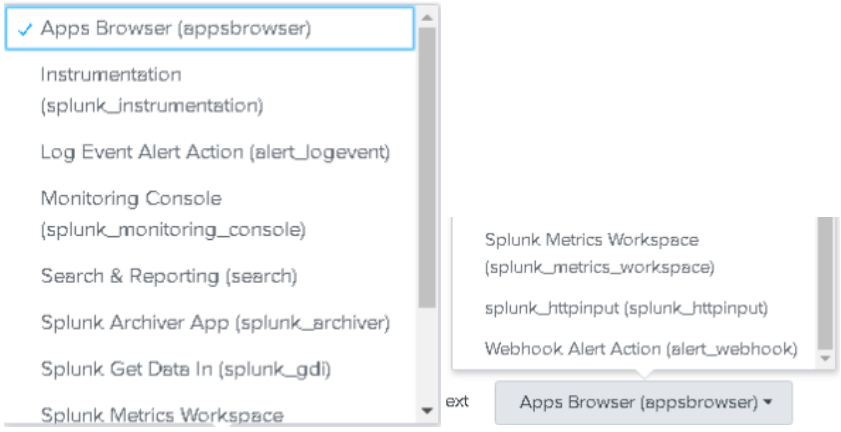
Con todos los datos listos hacemos clic en Next, luego con el botón New creamos un nuevo tipo de fuente de datos o Source Type, al cual denominamos Syslog Router Cisco. Tal como se muestra en la imagen que inicia en la siguiente página.



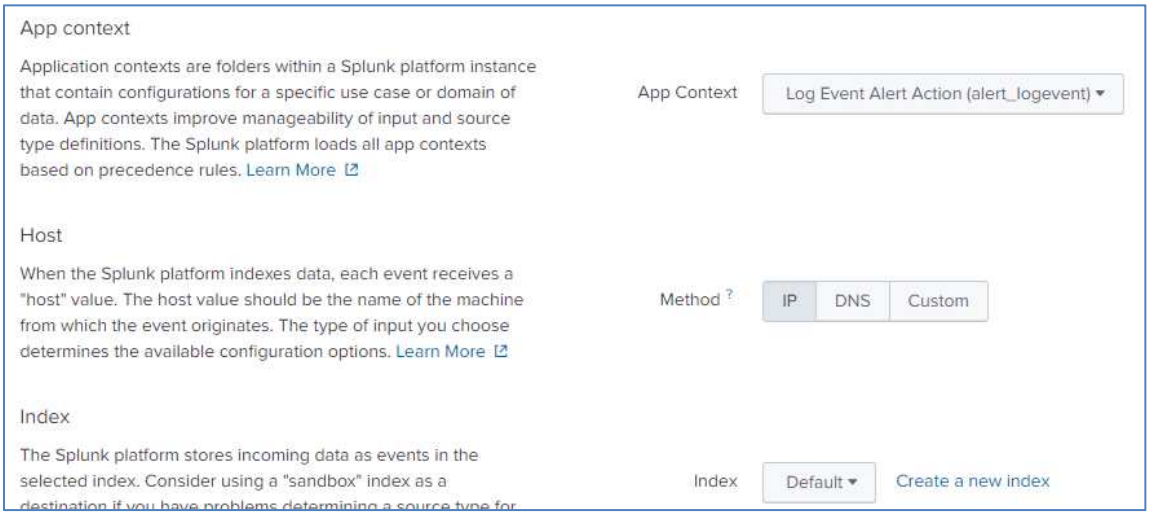
En este momento escribimos en el campo Source Type Syslog Router Cisco, en el campo Source Type Category seleccionamos de todas las categorías disponibles Network & Security y en Source Type Description escribimos la descripción Log de Router Cisco. Tal como se muestra en la siguiente imagen.



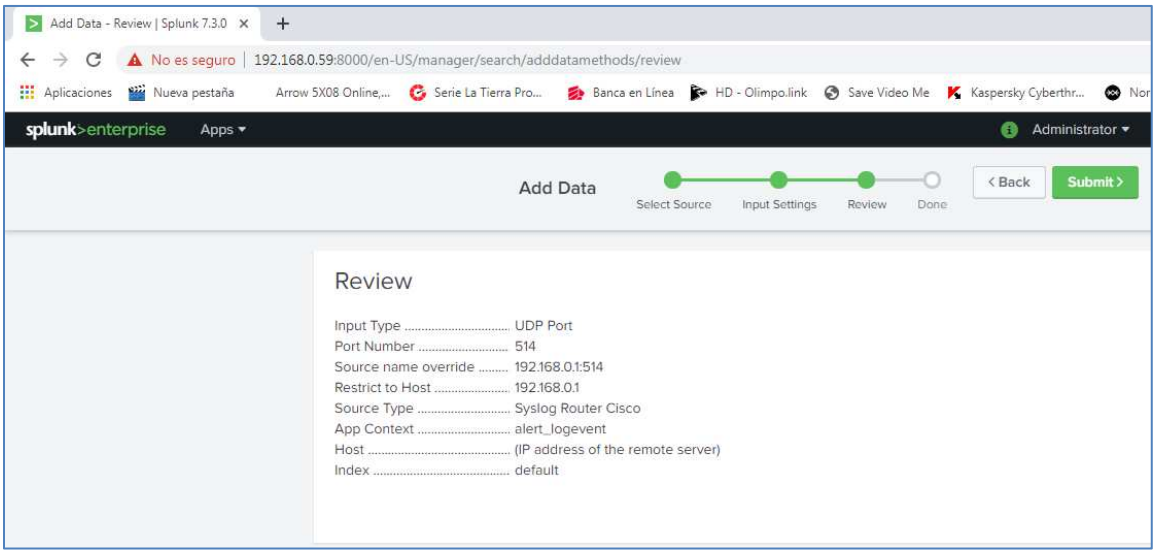
En la opción App Context se selecciona el contexto para el cual es utilizado el origen de datos remoto. En nuestro Caso seleccionamos Log Event Alert Action.



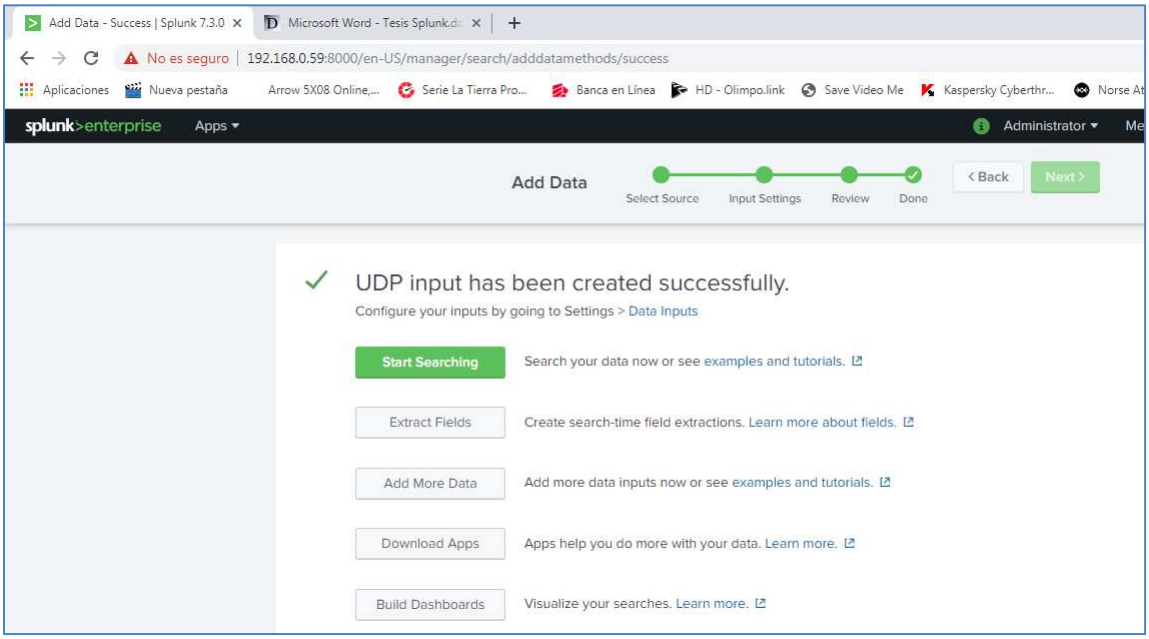
En el campo Method seleccionamos la opción IP puesto que es con el número IP del equipo que trabajamos. Finalmente en el campo Index seleccionamos Default. Hacemos clic en Next.



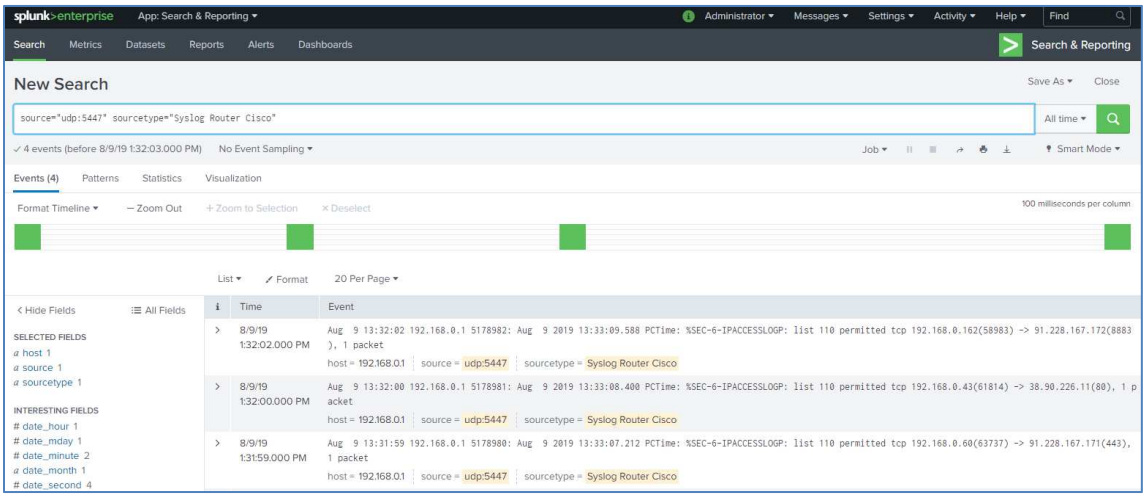
La penúltima etapa de configuración del Origen de Datos es la revisión de todo lo configurado. Luego hacemos clic en Submit para añadir el origen de datos creados. Tal como se muestra en la siguiente página.



El resultado final es que ya podemos hacer clic en ver los datos obtenidos por el Splunk Enterprise en el origen de datos creado. Hacemos clic en Start Searching.



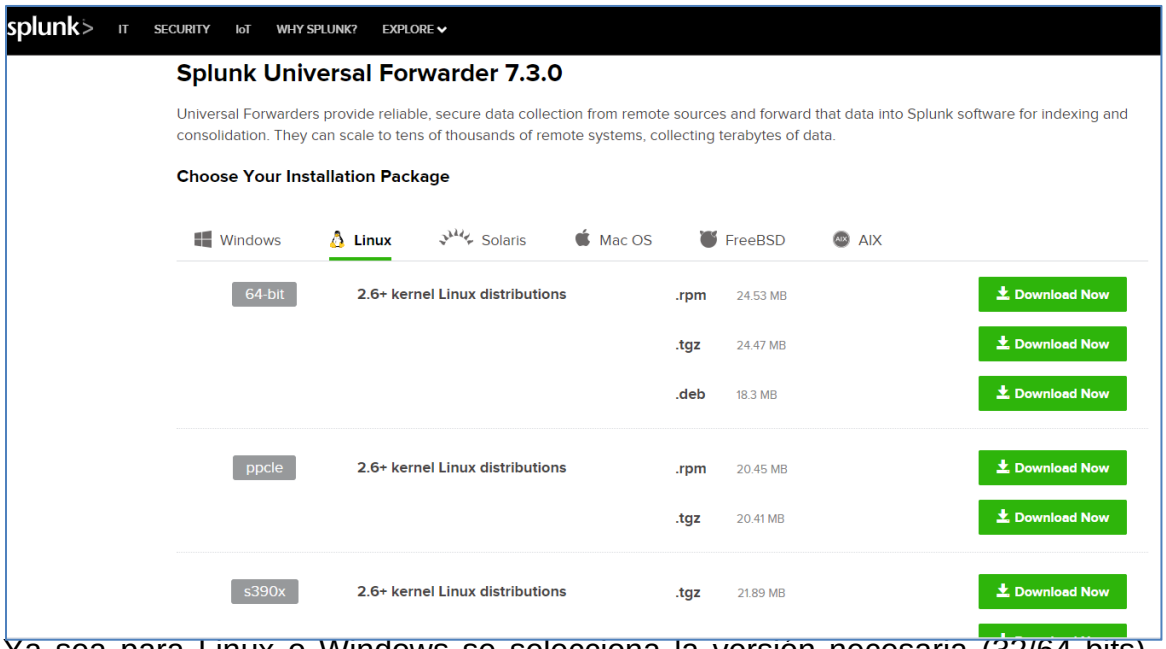
Ya se pueden observar los log generados por el Router en la imagen que se muestra al inicio de la página siguiente.



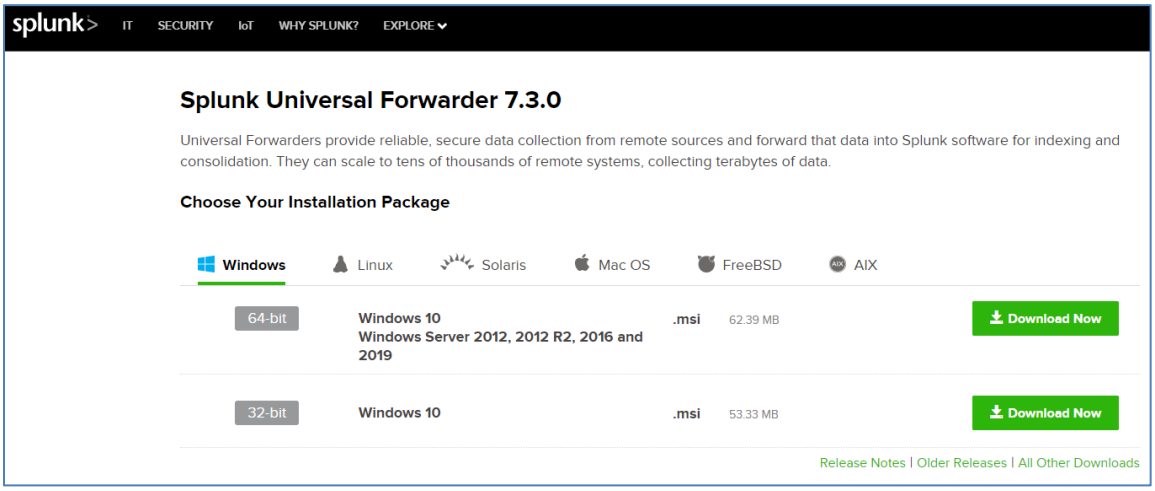
A esta información se le puede extraer campos y crear reglas específicas. Por ejemplo se puede crear reglas que indiquen cuando se realiza un telnet o ssh a un IP especifico.

Otro elemento importante a integrar son servidores tanto Windows como Linux. Los métodos de integración anterior son útiles para equipos de red (Switches, Routers, UTM). Para el caso de servidores se utilizan los llamados reenviadores o en ingles Forwarders.

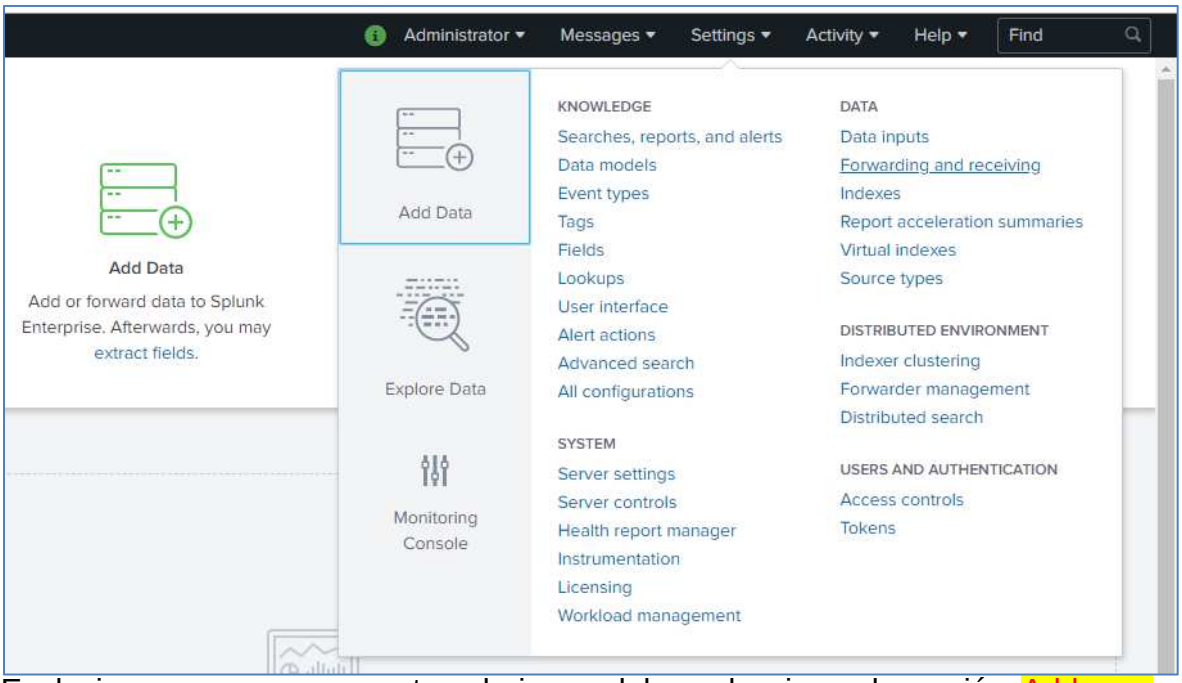
Para emplear forwarders se descargan para el sistema operativo requerido del sitio de splunk (www.splunk.com/en_us/download/universal-forwarder.html). Se ingresa con el usuario creado para las descargas de splunk. Tal como se muestra en la imagen que inicia en la siguiente página.



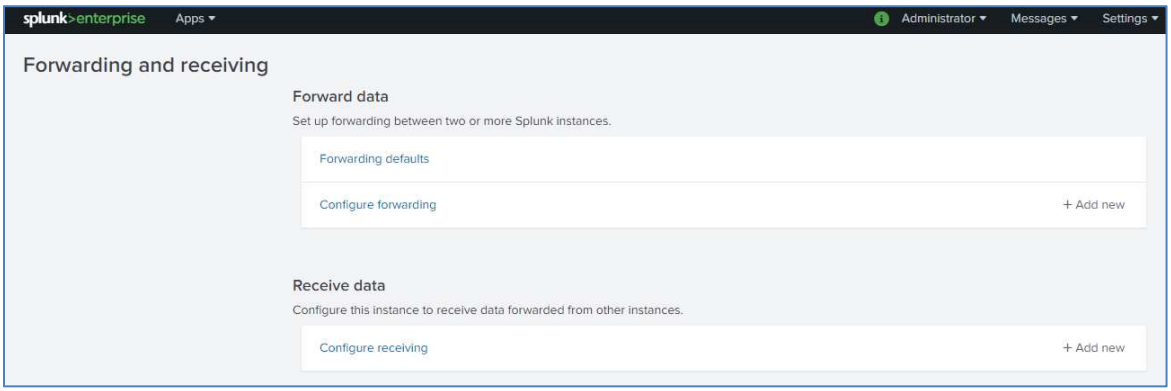
Ya sea para Linux o Windows se selecciona la versión necesaria (32/64 bits).



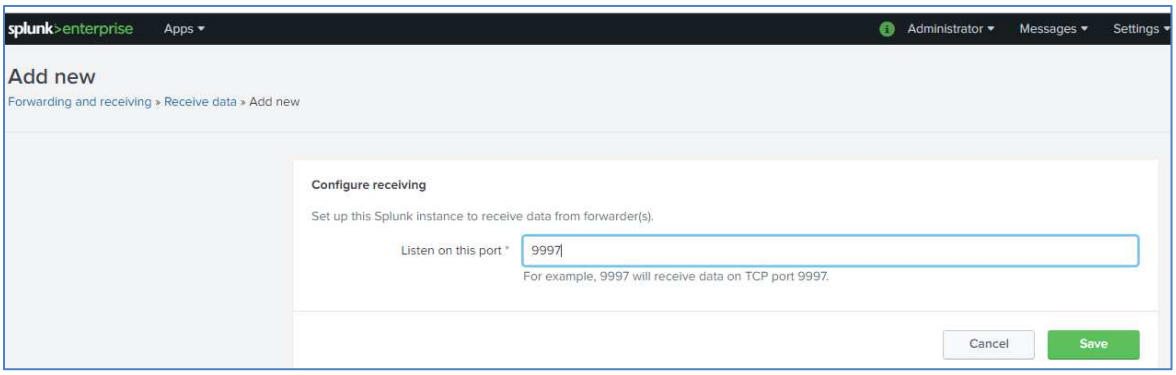
Para la instalación de los paquetes en Windows es sencillo. Basta con hacer clic en siguiente o Next en cada etapa y una vez instalado el paquete verificar en agregar o quitar programas. Luego en splunk ya se está listo para iniciar el proceso. En Settings seleccionar ir a Data y seleccionar la opción Forwarding and receiving. Tal como se muestra en la imagen que inicia en la página siguiente.



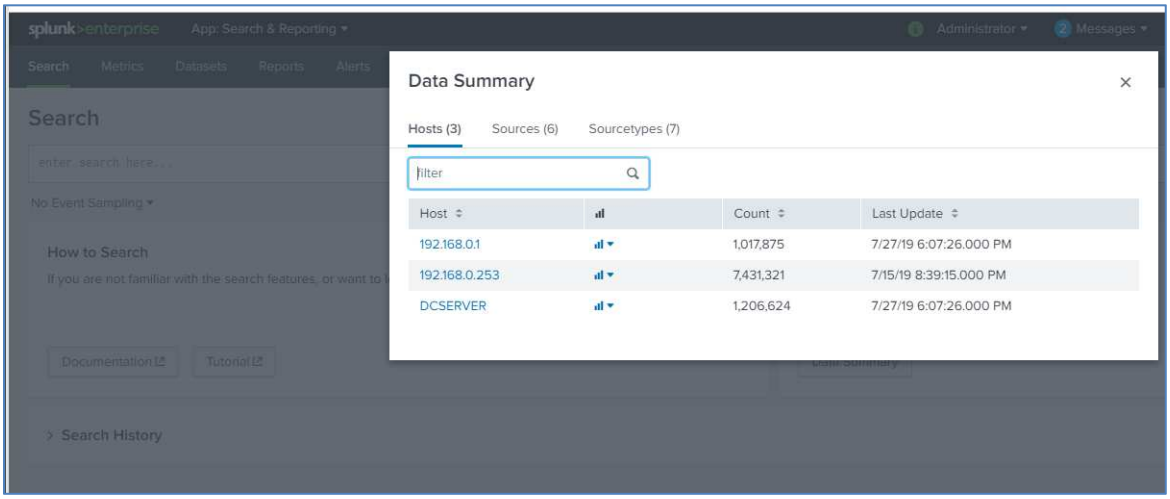
En la imagen que se muestra abajo se debe seleccionar la opción Add new dentro de Receive data para configurar el puerto del servidor de reenvío de LOG.



Ahora escribimos el puerto por defecto que utilizan los reenviadores de splunk, que es 9997, tal como se muestra en la imagen que inicia en la página siguiente.

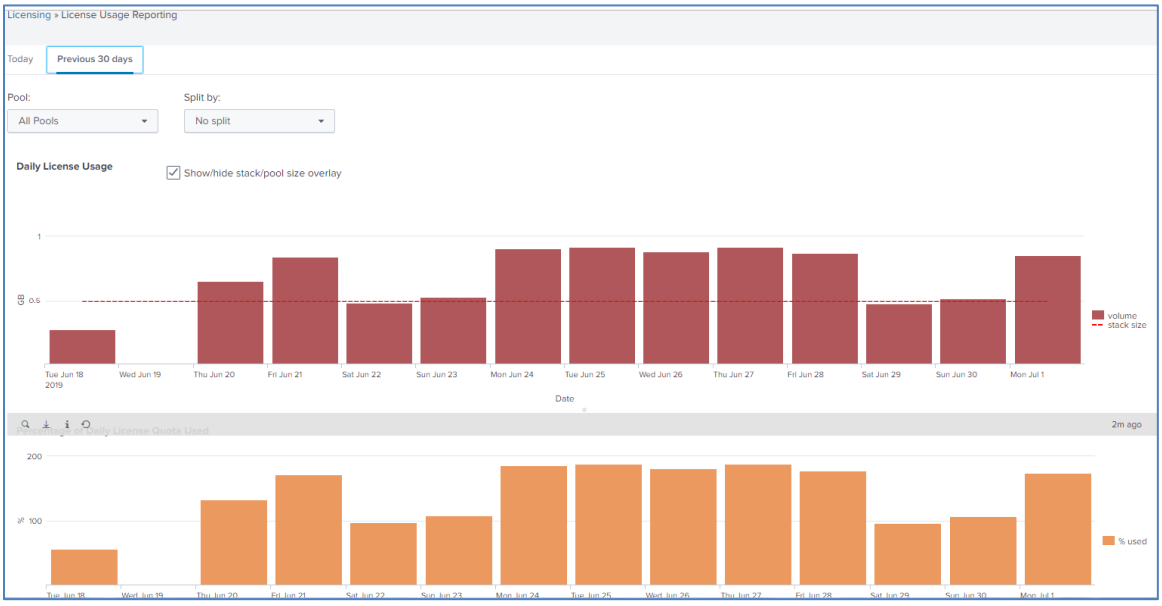


En este caso simplemente le damos guardar y nuestro servidor de Splunk está listo para recibir los LOG. La siguiente imagen muestra los dispositivos que están enviando LOG al Splunk Enterprise.



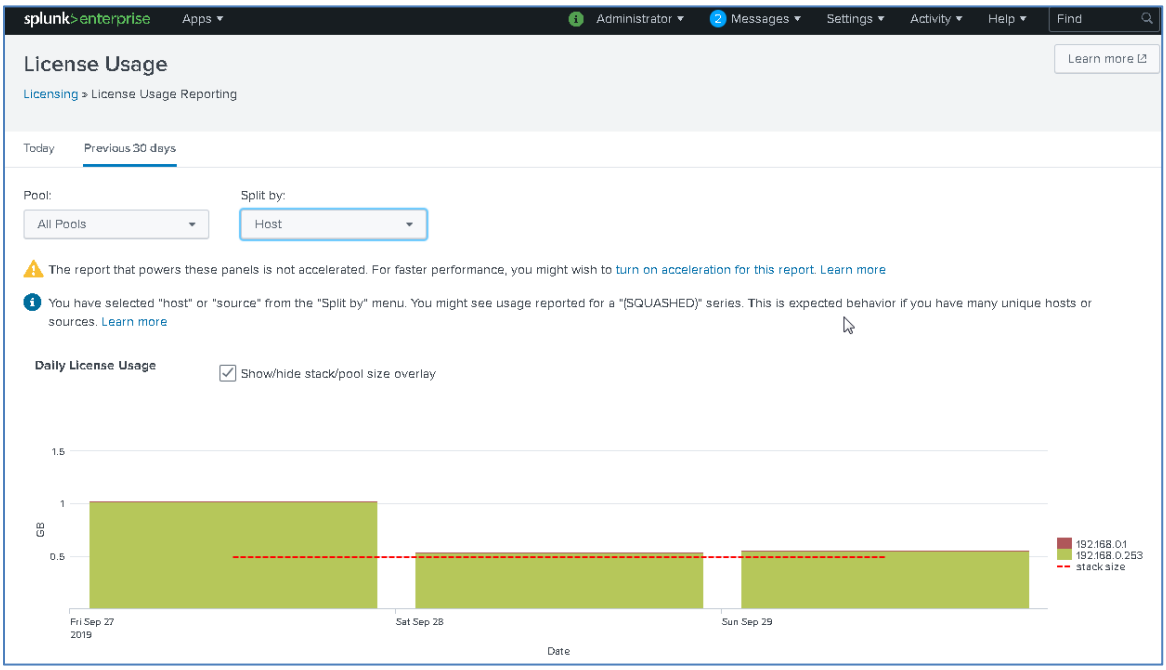
A-3. volumen de LOG generados por principales equipos de la red.

A partir del momento que se instaló Splunk se ha llevado un seguimiento de la cantidad de LOG que generan los equipos. En las siguientes imágenes se puede observar que en una licencia para 500 MB por día siempre se está superando hasta el doble. Tal como se muestra en la imagen que sigue.



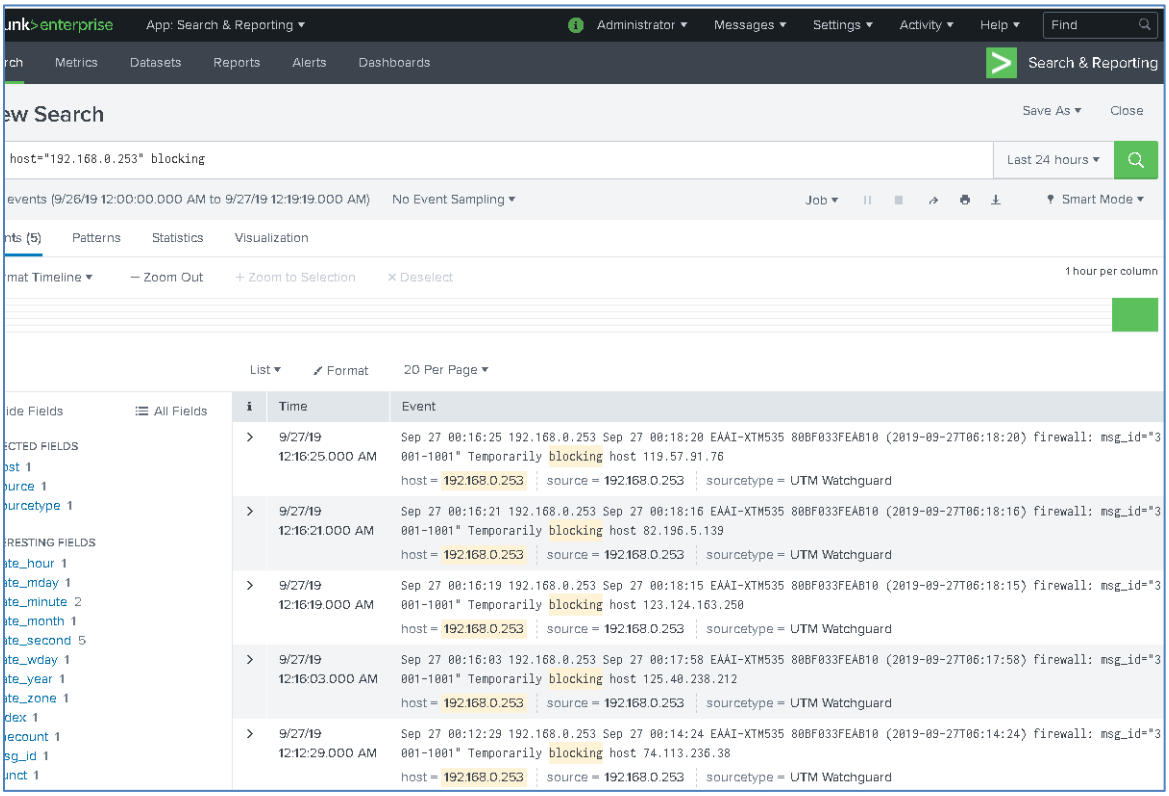
En la imagen anterior se observa que en el transcurso de una semana los LOG generados por dos equipos (un Router y un UTM) supera la licencia. De igual forma se confirma a nivel de porcentaje en la siguiente imagen.

La imagen que se describe a continuación brinda un resumen de tres días para dos equipos. En donde se observa que solo el fin de semana la licencia es superada por unos 100 MB. En el tráfico diario se supera por 500 MB. El UTM es el que más licencia consume.



A-4. Ejemplos de Alertas y búsquedas en Splunk

La siguiente imagen muestra una simple búsqueda en la que se consulta si el UTM ha bloqueado a alguien. La simple búsqueda **host="192.168.0.253" blocking** , da como resultado todo lo que el UTM está bloqueando. Si seleccionamos la opción Save As podemos elegir entre crear reporte o alerta

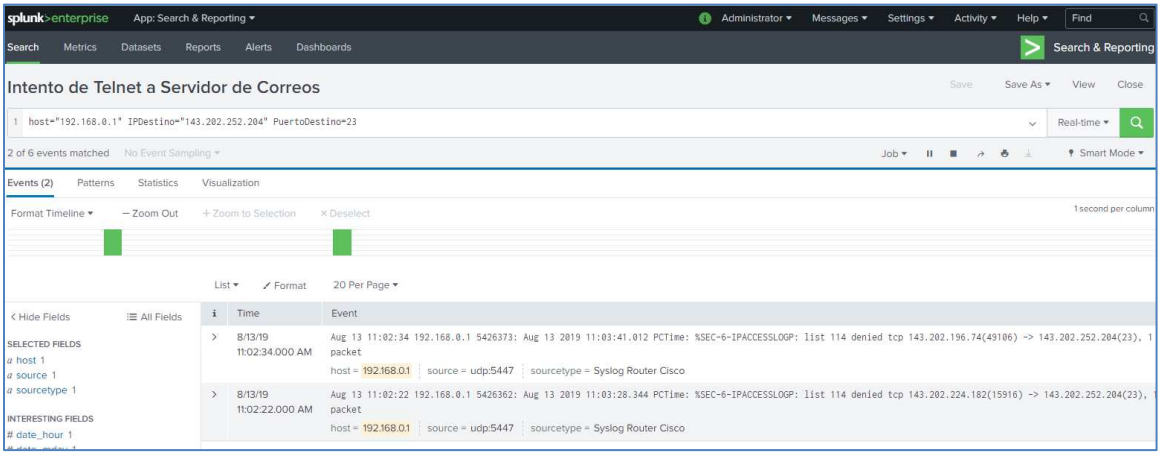


Podemos hacer otro tipo de consultas al equipo que deseemos. Simplemente hay que saber por ejemplo en cada LOG a que lista de acceso en el caso del Router se tiene datos de la LAN, WAN o VPN.

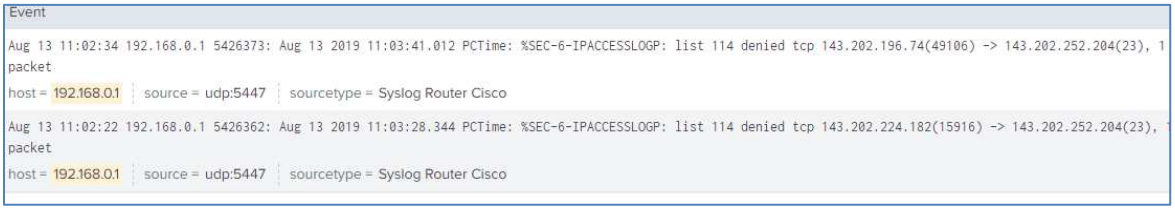
Si deseamos saber quién está haciendo telnet al servidor de correos públicos le preguntamos al Router en una alerta ya creada quien está intentando conectarse al puerto 23 del servidor. Así como puede ser el 23 podemos seleccionar el SSH (22). La búsqueda realizada es:

```
1  host="192.168.0.1" IPDestino="143.202.252.204" PuertoDestino=23
```

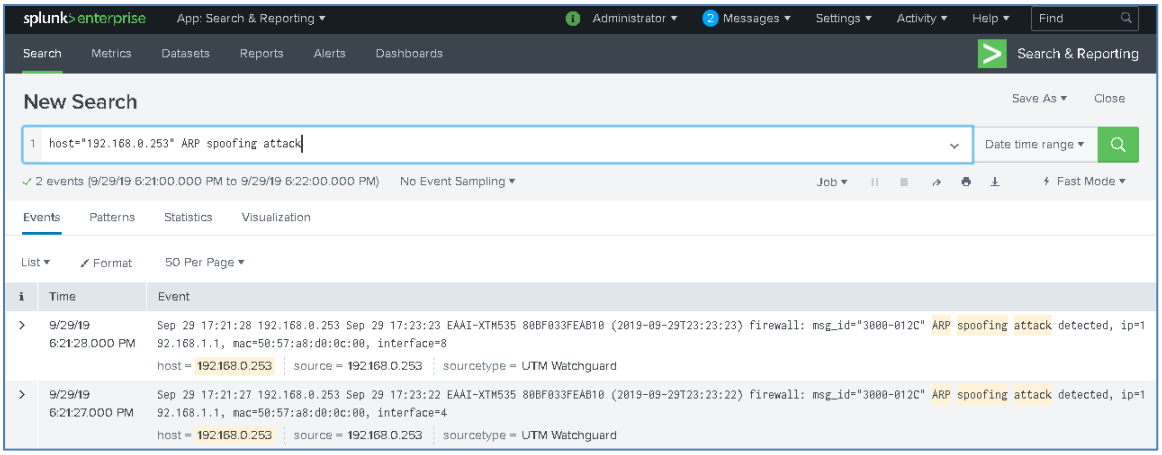
Al realizar la búsqueda expuesta de equipos que desean conectarse al puerto 23 del IP Destino 143.202.252.204 se puede utilizar por medio de filtros para crear alertas emergentes en pantalla o por correo. A continuación el resultado de la búsqueda programada como alerta de correos con el patrón de búsqueda de la página anterior.



Esta alerta se programa en el tiempo que uno dese y se puede enviar por correo. Los campos IPDestino y PuertoDestino fueron agregados de forma manual en un proceso de extracción de datos que brinda Splunk. En conclusión esta información mostrada abajo resulta útil pues podemos bloquear el IP Publico que intenta ingresar a nuestro equipo con un telnet o cualquier puerto conocido par afines de administración o conexión remota. Aunque no pueda hacerlo porque el Router lo está bloqueando. Pero es un buen indicio para tenerlos en una lista negra de posibles atacantes.

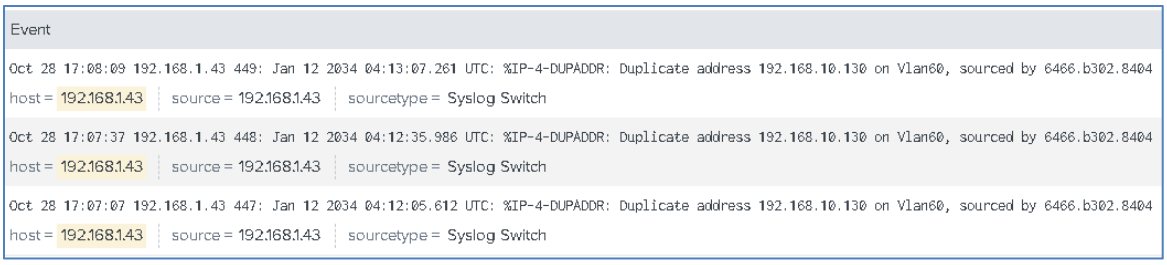


Ejemplo de búsqueda para Detección de ataque ARP (Suplantación de MAC o IP)

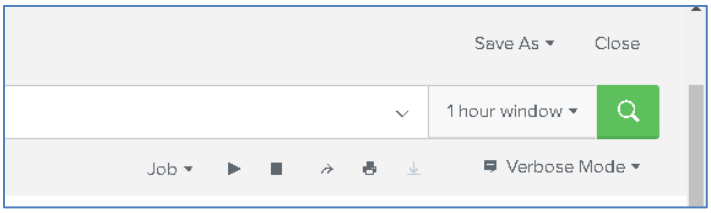


Búsqueda de MAC Duplicados

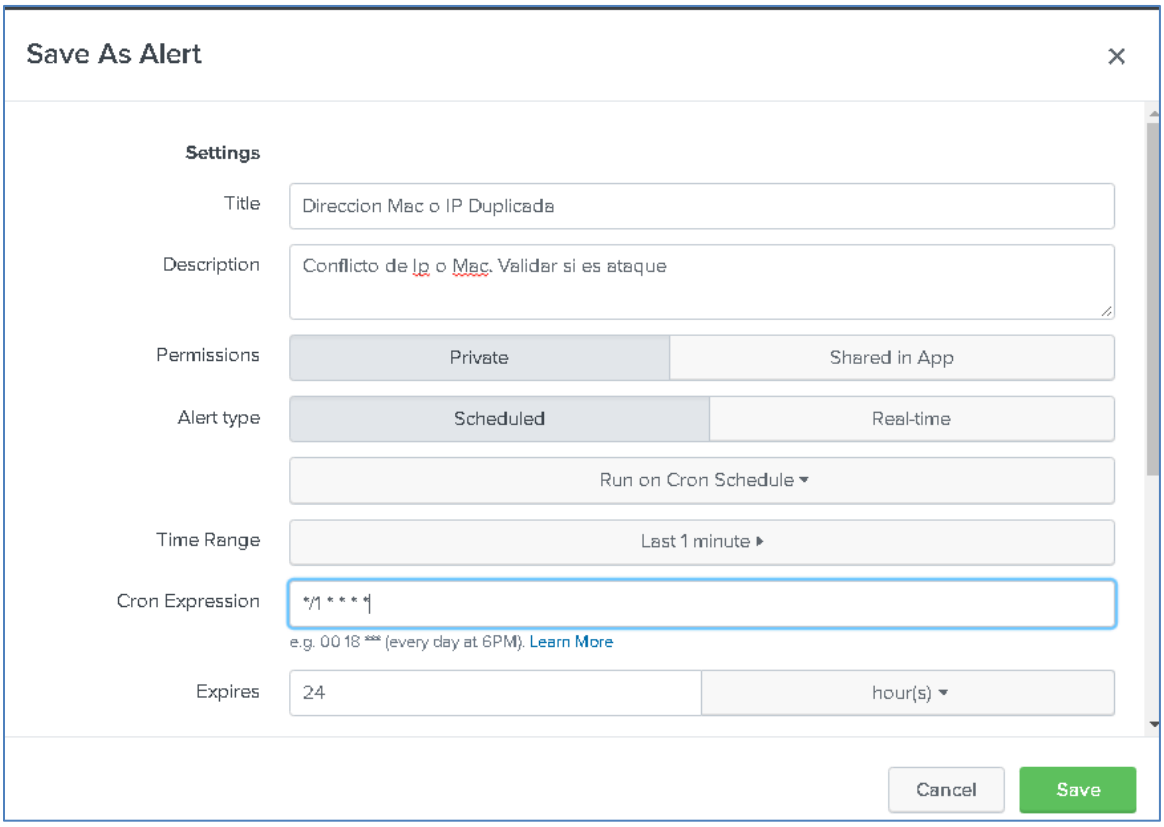
En este caso se realiza una búsqueda con el siguiente dato: **host=”192.168.1.43” Duplicate**. El resultado es la imagen siguiente.



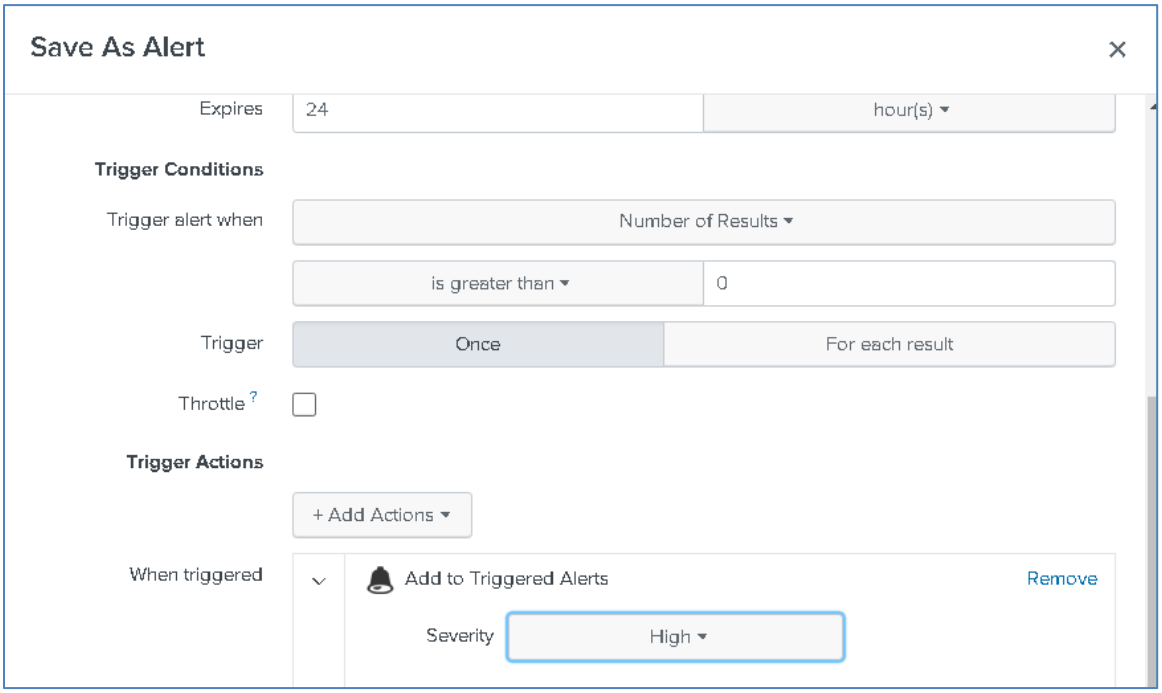
En la opción Save As se elige Save as Alert (Guardar como Alerta).



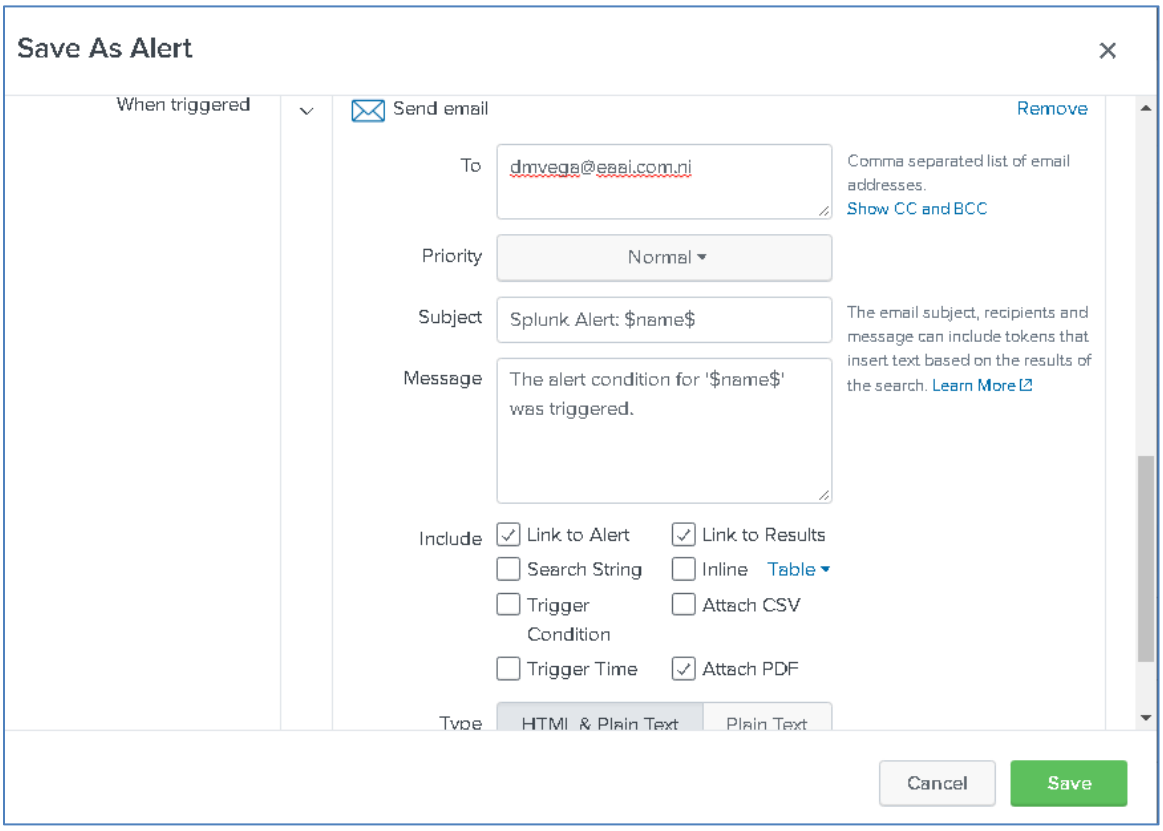
El primer campo a llenar es título de la alerta, luego se establece que es un tipo de alerta programada, se programa para revisión cada minuto. Se inicializa cada día. Tal como se muestra en la figura inicial de la página siguiente.



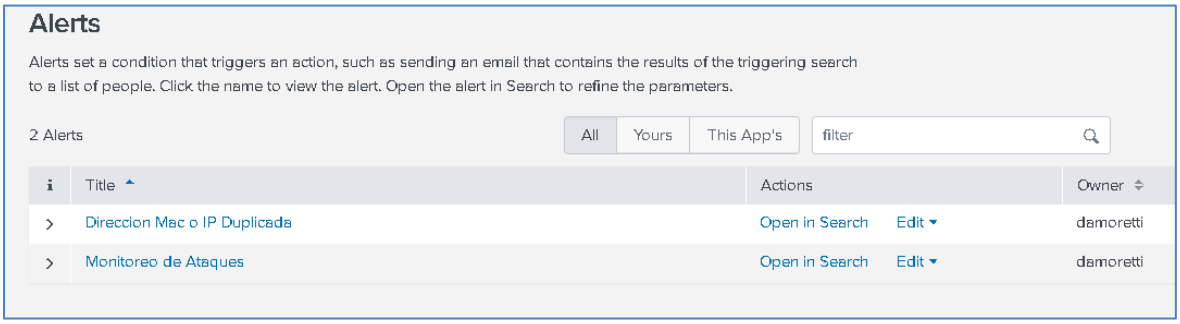
Casi al final en la parte de abajo se agrega un disparador (Trigger) que realice notificación en registro de eventos. Tal como se muestra en la imagen que sigue.



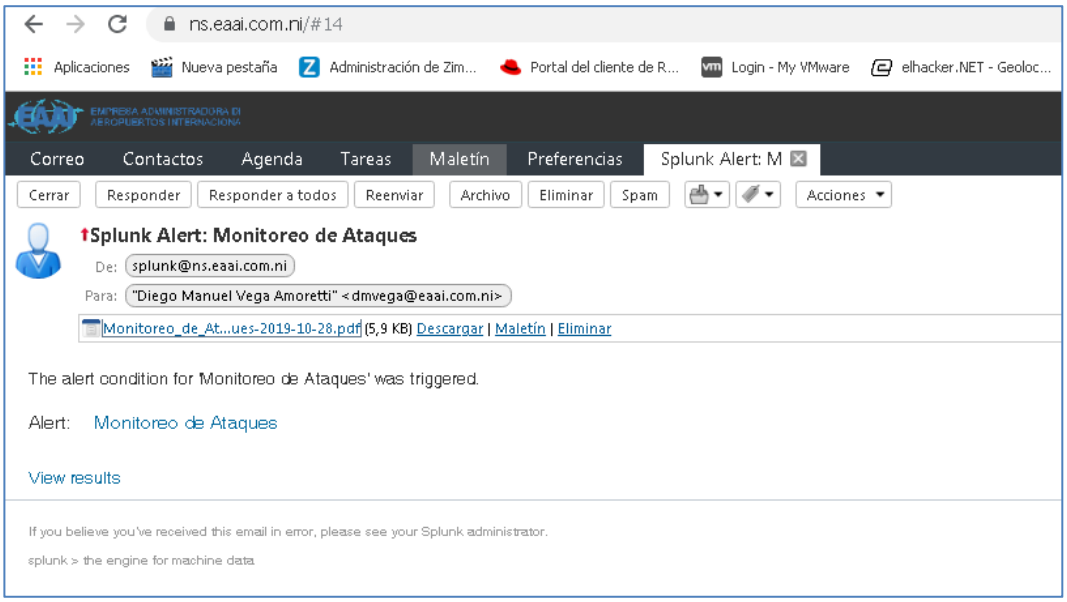
Luego se agrega otra acción del tipo disparador (Trigger) para también tener opción de enviar por correo la alerta. Se escribe en el campo To la dirección de correo, si se desea se establece una prioridad, luego se marca que se adjuntó el informe en PDF.



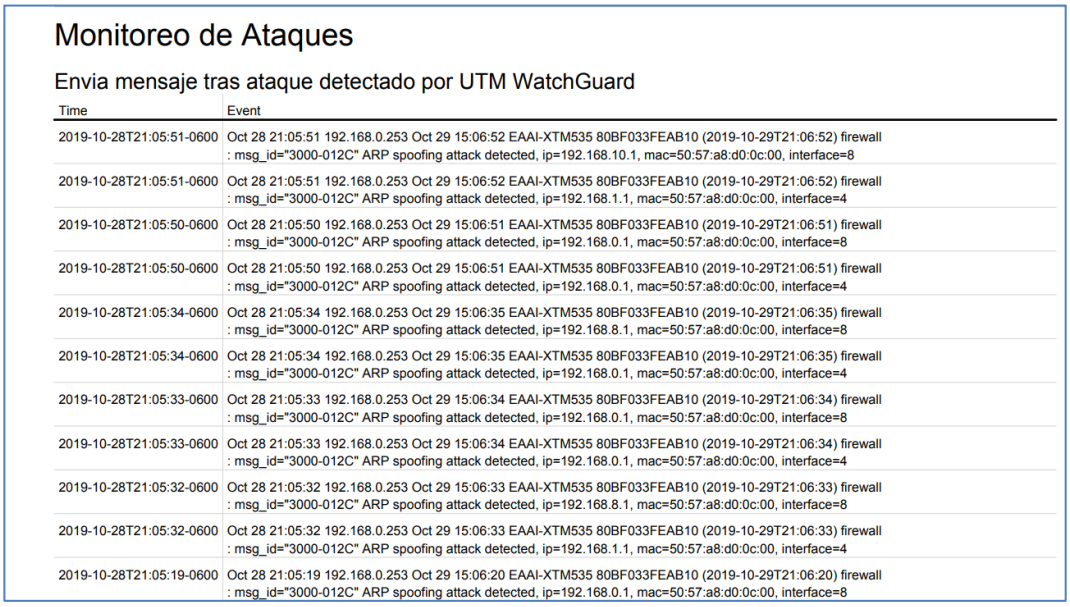
Finalmente hacemos clic en Save para salvar la alerta. En la imagen de abajo podemos ver las alertas que se han creado.



A continuación en la imagen que sigue se muestra información de un ejemplo de ataque de suplantación de MAC. Este ha sido enviado por correo electrónico a la cuenta dmvega@eaai.com.ni.



Cuando abrimos el PDF el resultado es todas las notificaciones registradas con datos de MAC del equipo atacante. Tal como se muestra abajo.



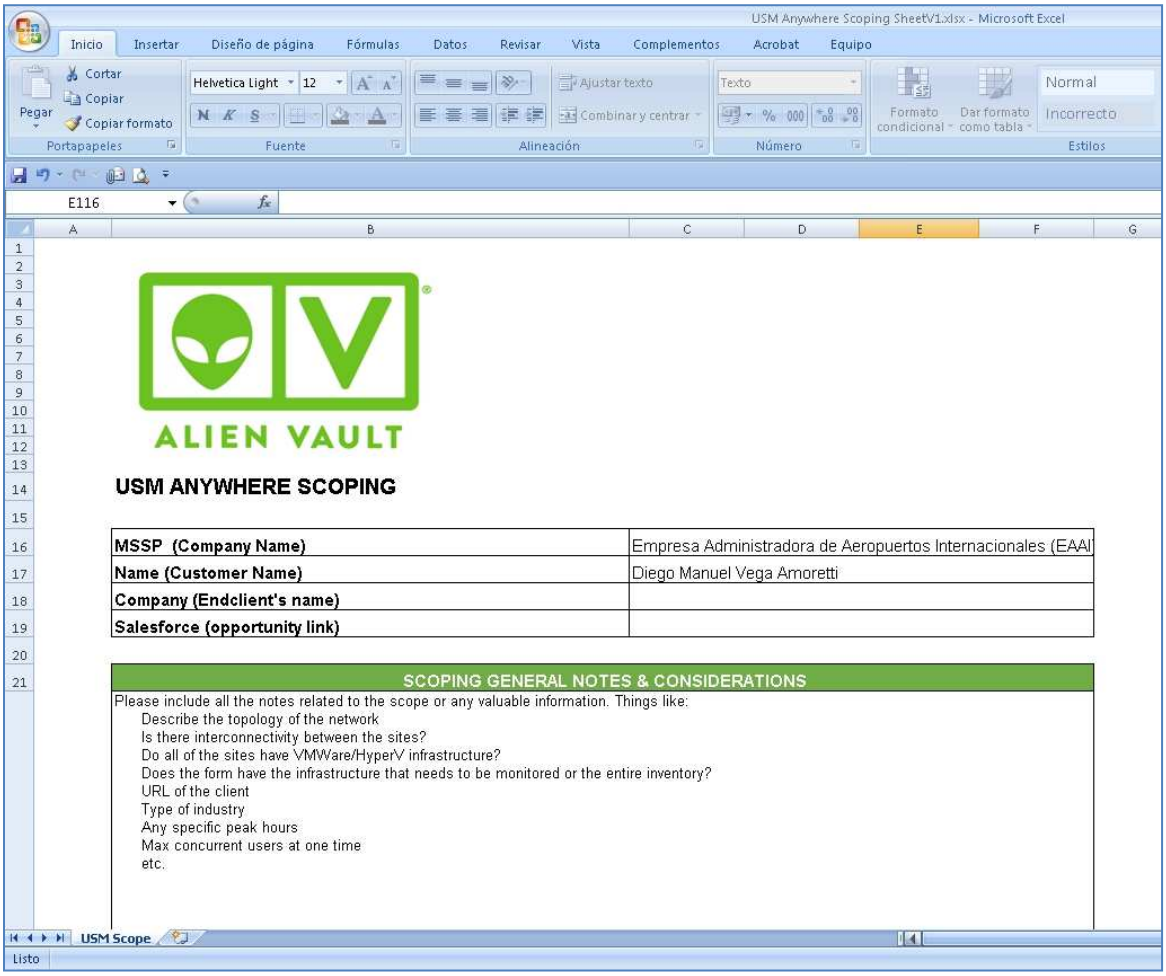
Monitoreo de Ataques

Envia mensaje tras ataque detectado por UTM WatchGuard

Time	Event
2019-10-28T21:05:51-0600	Oct 28 21:05:51 192.168.0.253 Oct 29 15:06:52 EAAI-XTM535 80BF033FEAB10 (2019-10-29T21:06:52) firewall : msg_id="3000-012C" ARP spoofing attack detected, ip=192.168.10.1, mac=50:57:a8:d0:0c:00, interface=8
2019-10-28T21:05:51-0600	Oct 28 21:05:51 192.168.0.253 Oct 29 15:06:52 EAAI-XTM535 80BF033FEAB10 (2019-10-29T21:06:52) firewall : msg_id="3000-012C" ARP spoofing attack detected, ip=192.168.1.1, mac=50:57:a8:d0:0c:00, interface=4
2019-10-28T21:05:50-0600	Oct 28 21:05:50 192.168.0.253 Oct 29 15:06:51 EAAI-XTM535 80BF033FEAB10 (2019-10-29T21:06:51) firewall : msg_id="3000-012C" ARP spoofing attack detected, ip=192.168.0.1, mac=50:57:a8:d0:0c:00, interface=8
2019-10-28T21:05:50-0600	Oct 28 21:05:50 192.168.0.253 Oct 29 15:06:51 EAAI-XTM535 80BF033FEAB10 (2019-10-29T21:06:51) firewall : msg_id="3000-012C" ARP spoofing attack detected, ip=192.168.0.1, mac=50:57:a8:d0:0c:00, interface=4
2019-10-28T21:05:34-0600	Oct 28 21:05:34 192.168.0.253 Oct 29 15:06:35 EAAI-XTM535 80BF033FEAB10 (2019-10-29T21:06:35) firewall : msg_id="3000-012C" ARP spoofing attack detected, ip=192.168.8.1, mac=50:57:a8:d0:0c:00, interface=8
2019-10-28T21:05:34-0600	Oct 28 21:05:34 192.168.0.253 Oct 29 15:06:35 EAAI-XTM535 80BF033FEAB10 (2019-10-29T21:06:35) firewall : msg_id="3000-012C" ARP spoofing attack detected, ip=192.168.0.1, mac=50:57:a8:d0:0c:00, interface=4
2019-10-28T21:05:33-0600	Oct 28 21:05:33 192.168.0.253 Oct 29 15:06:34 EAAI-XTM535 80BF033FEAB10 (2019-10-29T21:06:34) firewall : msg_id="3000-012C" ARP spoofing attack detected, ip=192.168.0.1, mac=50:57:a8:d0:0c:00, interface=8
2019-10-28T21:05:33-0600	Oct 28 21:05:33 192.168.0.253 Oct 29 15:06:34 EAAI-XTM535 80BF033FEAB10 (2019-10-29T21:06:34) firewall : msg_id="3000-012C" ARP spoofing attack detected, ip=192.168.0.1, mac=50:57:a8:d0:0c:00, interface=4
2019-10-28T21:05:32-0600	Oct 28 21:05:32 192.168.0.253 Oct 29 15:06:33 EAAI-XTM535 80BF033FEAB10 (2019-10-29T21:06:33) firewall : msg_id="3000-012C" ARP spoofing attack detected, ip=192.168.8.1, mac=50:57:a8:d0:0c:00, interface=8
2019-10-28T21:05:32-0600	Oct 28 21:05:32 192.168.0.253 Oct 29 15:06:33 EAAI-XTM535 80BF033FEAB10 (2019-10-29T21:06:33) firewall : msg_id="3000-012C" ARP spoofing attack detected, ip=192.168.1.1, mac=50:57:a8:d0:0c:00, interface=4
2019-10-28T21:05:19-0600	Oct 28 21:05:19 192.168.0.253 Oct 29 15:06:20 EAAI-XTM535 80BF033FEAB10 (2019-10-29T21:06:20) firewall : msg_id="3000-012C" ARP spoofing attack detected, ip=192.168.0.1, mac=50:57:a8:d0:0c:00, interface=8

A-5. Formulario para Precio AlienVault

Lo que a continuacion se muestra es un cuestionario que se llenó para AlienVault con propositos de dimencinonar el precio de la solución SIEM AlienVault USM



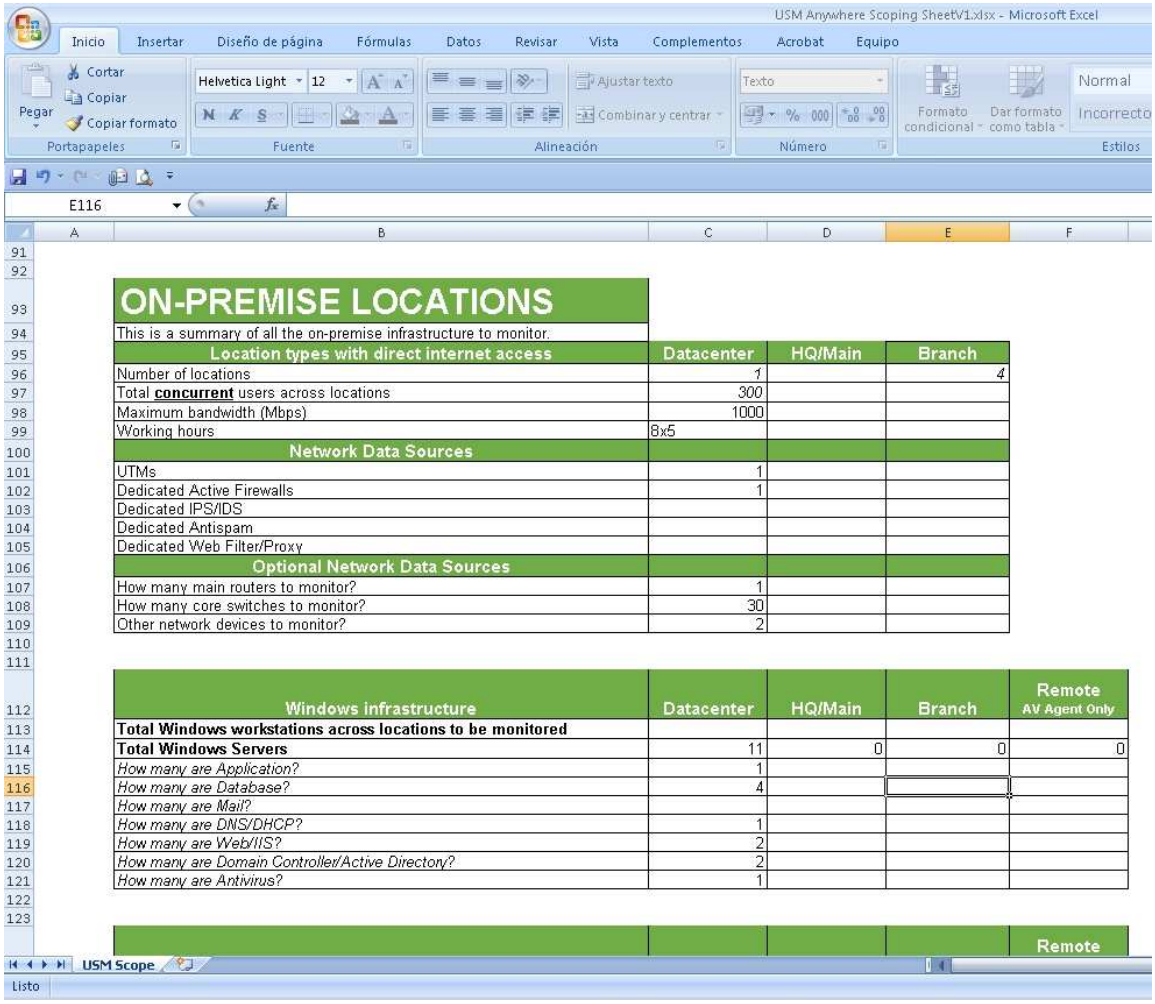
USM Anywhere Scoping SheetV1.xlsx - Microsoft Excel

ALIEN VAULT

USM ANYWHERE SCOPING

MSSP (Company Name)	Empresa Administradora de Aeropuertos Internacionales (EAAI
Name (Customer Name)	Diego Manuel Vega Amoretti
Company (Endclient's name)	
Salesforce (opportunity link)	

SCOPING GENERAL NOTES & CONSIDERATIONS
Please include all the notes related to the scope or any valuable information. Things like: Describe the topology of the network Is there interconnectivity between the sites? Do all of the sites have VMWare/HyperV infrastructure? Does the form have the infrastructure that needs to be monitored or the entire inventory? URL of the client Type of industry Any specific peak hours Max concurrent users at one time etc.



USM Anywhere Scoping SheetV1.xlsx - Microsoft Excel

Inicio | Insertar | Diseño de página | Fórmulas | Datos | Revisar | Vista | Complementos | Acrobat | Equipo

Cortar | Copiar | Copiar formato | Pegar | Portapapeles | Helvetica Light | 12 | Fuente | Ajustar texto | Combinar y centrar | Alineación | Texto | Número | Formato condicional | Dar formato como tabla | Normal | Incorrecto | Estilos

E116

ON-PREMISE LOCATIONS

This is a summary of all the on-premise infrastructure to monitor.

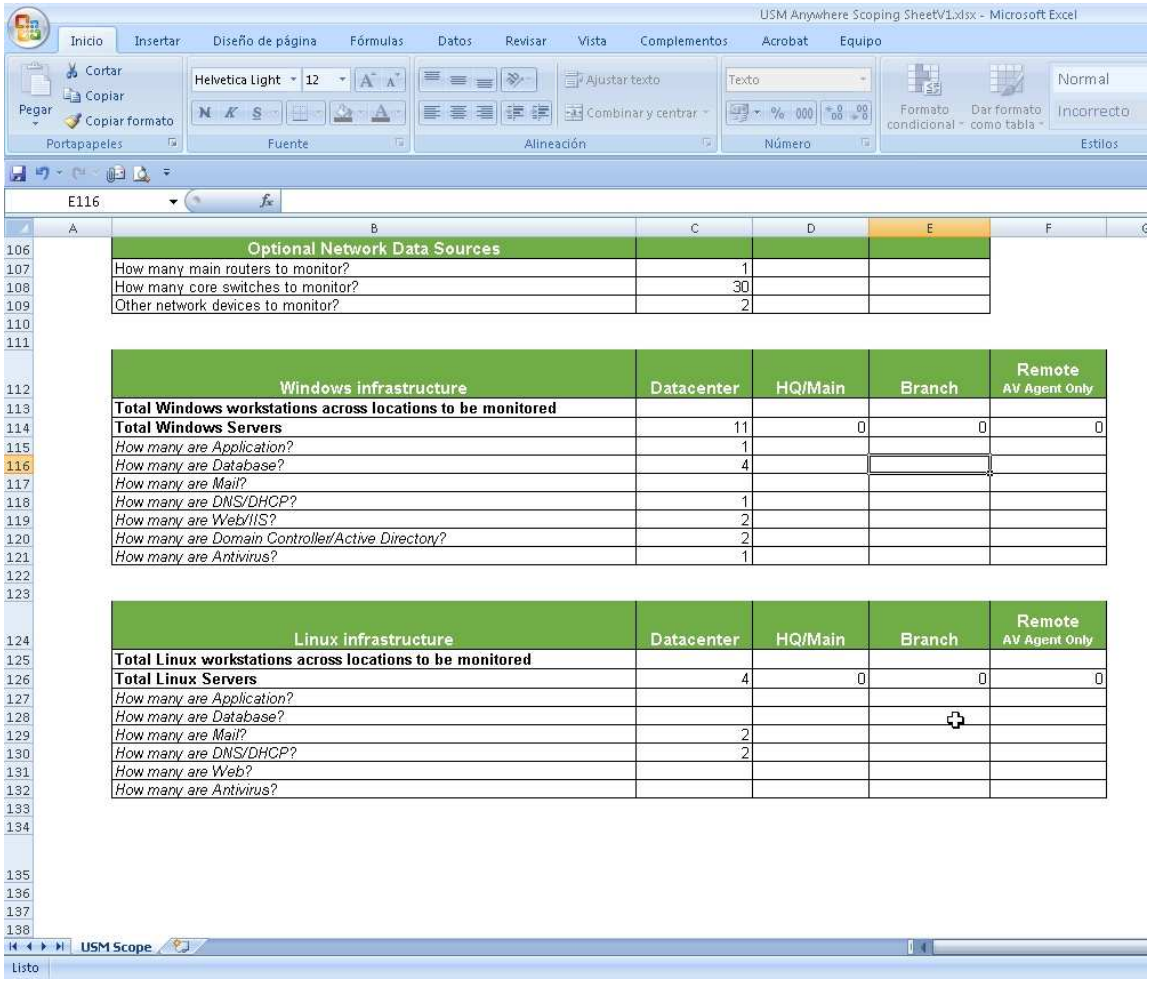
Location types with direct internet access	Datacenter	HQ/Main	Branch
Number of locations	*1*		*4*
Total **concurrent** users across locations	*300*		
Maximum bandwidth (Mbps)	1000		
Working hours	8x5		
Network Data Sources			
UTMs	1		
Dedicated Active Firewalls	1		
Dedicated IPS/IDS			
Dedicated Antispam			
Dedicated Web Filter/Proxy			
Optional Network Data Sources			
How many main routers to monitor?	1		
How many core switches to monitor?	30		
Other network devices to monitor?	2		

Windows infrastructure	Datacenter	HQ/Main	Branch	Remote AV Agent Only
Total Windows workstations across locations to be monitored				
Total Windows Servers	11	0	0	0
How many are Application?	1			
How many are Database?	4			
How many are Mail?				
How many are DNS/DHCP?	1			
How many are Web/IIS?	2			
How many are Domain Controller/Active Directory?	2			
How many are Antivirus?	1			

				Remote

USM Scope

Listo



USM Anywhere Scoping SheetV1.xlsx - Microsoft Excel

Optional Network Data Sources				
How many main routers to monitor?	1			
How many core switches to monitor?	30			
Other network devices to monitor?	2			

Windows infrastructure	Datacenter	HQ/Main	Branch	Remote AV Agent Only
Total Windows workstations across locations to be monitored				
Total Windows Servers	11	0	0	0
How many are Application?	1			
How many are Database?	4			
How many are Mail?				
How many are DNS/DHCP?	1			
How many are Web/IIS?	2			
How many are Domain Controller/Active Directory?	2			
How many are Antivirus?	1			

Linux infrastructure	Datacenter	HQ/Main	Branch	Remote AV Agent Only
Total Linux workstations across locations to be monitored				
Total Linux Servers	4	0	0	0
How many are Application?				
How many are Database?				
How many are Mail?	2			
How many are DNS/DHCP?	2			
How many are Web?				
How many are Antivirus?				

La solución de AlienVaulT USM fue calculada para: 300 usuarios, 11 Servidores Windows, 4 Linux, 30 Switch, 1 UTM, 1 Router, 1 Firewall y 2 Dispositivos de Red.

Como Resultado el personal de AlienVault dimensionó la solución con los siguientes datos:

4/30/2019 USM Anywhere Scoping

ALIEN VAULT

USM Anywhere Scoping

Summary

Diego Manuel Vega Amoretti - Empresa Administradora de Aeropuertos Internacionales (EAAI)

► On-Premises Sensors: 1
257.835 GiB/Month
279 average EPS

▼ Environment Details: 8x5 | environment

Users: 300 | Endpoints: 300
Compliance Scope:

Total Estimated Data Consumption: 257.835 GiB/Month
Total Estimated EPS: 279

Minimum Tier: 250 GiB

Recommended Tier: 500 GiB

De tal forma que ofrece una solución para licenciar un equipo virtual local y con derecho a 250 GB por mes tanto local como en la nube. Se ofrece una solución hibrida. El total de usuarios contemplados son 300. Con una carga de hasta 279 EPS (Eventos por Segundo)

A-6. Campos Normalizados de OSSIM.

La siguiente lista de campos tanto en inglés como español son los que aparecen en todos los eventos ya normalizados.

Tabla de eventos normalizados y su descripción

Campos (Ingles)	Campos (Español)	Descripción
Date	Fecha	Fecha y hora del evento.
AlienVaultSensor	AlienVaultSensor	Sensor que procesó el evento.
Device IP	IP del dispositivo	Dirección IP del sensor del dispositivo USM/OSSIM que procesó el evento.
Event Type ID	ID del tipo de evento	ID asignado por el dispositivo USM/OSSIM para identificar el tipo de evento.
Unique Event ID#	ID de evento único #	Número de identificación único asignado al evento por USM/OSSIM Appliance (Dispositivo especializado).
Protocol	Protocolo	Protocolo utilizado para el origen / destino del evento, por ejemplo, TCP IP.
Category	Categoría	Taxonomía de eventos para el evento, por ejemplo, Autenticación o Explotación.
Sub-Category	Subcategoría	Subcategoría del tipo de taxonomía de eventos enumerada en Categoría. Por ejemplo, esto sería denegación de servicio, si la categoría fuera Exploit.
Data Source Name	Nombre de fuente de datos	Nombre de la aplicación o dispositivo externo que produjo el evento.
Data Source ID	ID de fuente de datos	ID asociado con la aplicación o dispositivo externo que produjo el evento.
Product Type	tipo de producto	Tipo de producto de la taxonomía de eventos, por ejemplo, Sistema operativo o Servidor. Nota: Los eventos con datos relacionados con la reputación de IP tienen tipos de productos, los pulsos OTX no.
Additional Info	Información adicional	Si el evento fuera generado por una URL sospechosa, por ejemplo, este campo indicaría la URL. Cuando están presentes, estas URL proporcionan información de fondo adicional y referencias sobre los componentes asociados con el evento.
Priority	Prioridad	Clasificación de prioridad, basada en el valor del tipo de evento. Cada tipo de evento tiene un valor de prioridad, utilizado en el cálculo del riesgo.

Reliability	Fiabilidad	Clasificación de confiabilidad, basada en el valor de confiabilidad del tipo de evento. Cada tipo de evento tiene un valor de confiabilidad, que se utiliza en el cálculo del riesgo.
Risk	Riesgo	Nivel de riesgo del evento: Bajo = 0, Medio = 1, Alto> 1. Nota: El cálculo del riesgo se basa en esta fórmula: Valor del activo * Confiabilidad del evento * Prioridad del evento / 25 = Riesgo Si el Valor del activo = 3, Confiabilidad = 2 y Prioridad = 2, el riesgo sería 3 * 2 * 2/25 = 0.48 (redondeado a 0). Por lo tanto, el riesgo es bajo
OTX Indicators	Indicadores OTX	Número de indicadores asociados con una reputación de IP o un evento de pulso OTX.
Source / Destination	Origen / Destino	Direcciones IP y nombre de host para el origen y el destino, respectivamente, del evento.
Hostname	Nombre de host	Es el nombre de host del origen o destino de un evento. Si el nombre de host de origen o destino para un evento está dentro de su inventario de activos, este campo contiene un valor.
MAC Address	Dirección MAC	Control de acceso a medios (MAC) del host para el evento, si se conoce.
Port	Puerto	Para la fuente de un evento de un activo interno o externo constituye el puerto.
Latest Update	Última actualización	La última vez que USM/OSSIM Appliance actualizó las propiedades del activo.
Username & Domain	Nombre de usuario y dominio	Nombre de usuario y dominio asociado con el activo que generó el evento.
Asset Value	Valor del activo	Es el valor de un activo del origen o destino del evento.
Location	Ubicación	Si se conoce el país de origen del anfitrión, muestra la bandera nacional del origen o destino del evento.

Context	Contexto	Si el activo pertenece a un grupo de entidades definido por el usuario, USM/OSSIM Appliance muestra los contextos.
Asset Groups	Grupos de activos	Cuando el host para el origen o destino del evento es un activo que pertenece a uno o más de sus grupos de activos, este campo enumera el nombre o los nombres del grupo de activos.
Networks	Redes	Cuando el host para el origen o destino del evento es un activo que pertenece a una o más de sus redes, este campo enumera las redes.
Logged Users	Usuarios registrados	Una lista de todos los usuarios que han estado activos en un equipo, según lo detectado por el escaneo del activo. Por ejemplo, con el nombre de usuario y el privilegio de usuario (como admin).
OTX IP Reputation	Reputación IP de OTX	(Sí / No) Si la reputación de IP identifica o no la dirección IP como sospechosa.
Service	Servicio	Lista de servicios o aplicaciones detectados en el puerto de origen / destino.
Port	Puerto	Puerto utilizado por el servicio o aplicación.
Protocol	Protocolo	Protocolo utilizado por el servicio o aplicación.
Raw Log	Registro sin procesar	Detalles de registro sin procesar del evento.

Otros Campos extras en la Normalización que se muestran en los eventos.

Campos (Ingles)	Campos (Español)	Descripción
Filename	Nombre del archivo	Nombre del archivo asociado con el evento.
Username	Nombre de usuario	El nombre de usuario asociado con el evento.
Password	Contraseña	La contraseña asociada al evento.
Userdata 1-9	Datos de usuario 1-9	Campos de registro creados por el usuario
Payload	Carga útil	Carga útil del evento.
Rule Detection	Detección de reglas	La regla AlienVault NIDS (Sistema de detección de intrusos de red) utilizada para detectar el evento.

A-7. Configuración de LOG Server

El equipo que actúa como LOG Server es un Centos 7. La configuración de la maquina virtual ya se mostró dentro del la instalación del OSSIM. Lo que a continuación se muestran son las pantallas de configuración del servicio rsyslog. Lo primero que se hizo fue preparar el disco duro que se dejo para LOG. Para esto empleamos el siguiente comando:

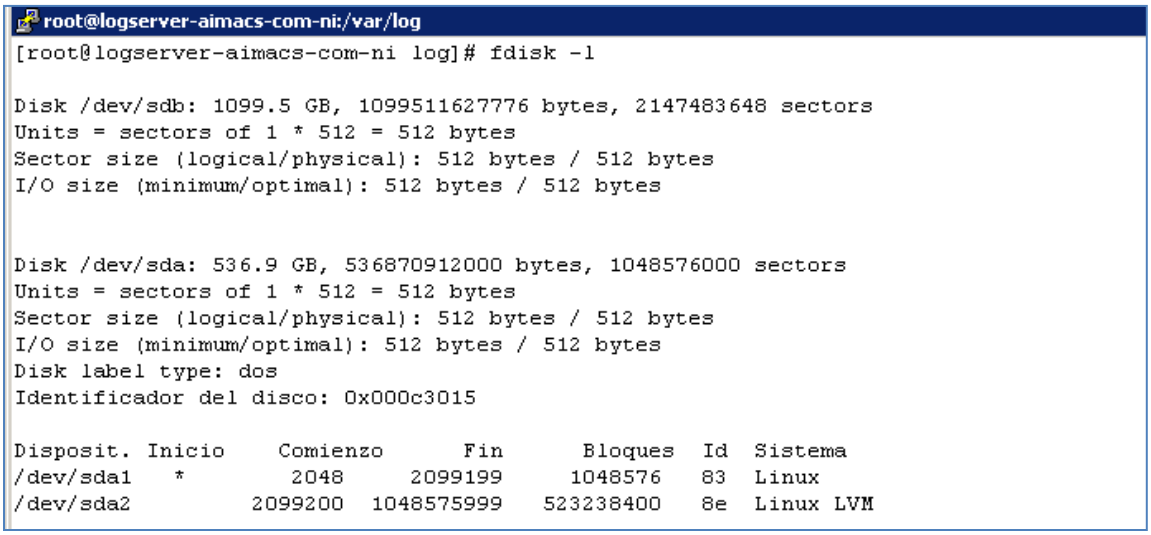
fdisk –l /* Para listar los discos existentes*/

Preparamos particiones y sistema de sistema de archivos

fdisk /dev/sdb

mkfs -t ext4 /dev/sdb

La siguiente imagen muestra el sistema de archivo ya listo.



En la partición sda2 está el espacio destinado para el LOG.

En la partición creada con sistema de archivos ext4 se guardaran todos los LOG. Para eso creamos un directorio en la raíz del Centros llamado LogServer para guardar todos los LOG una vez que montemos la partición ya lista. Los comandos ejecutados fueron:

mkdir /LogServer /* Crear directorio*/

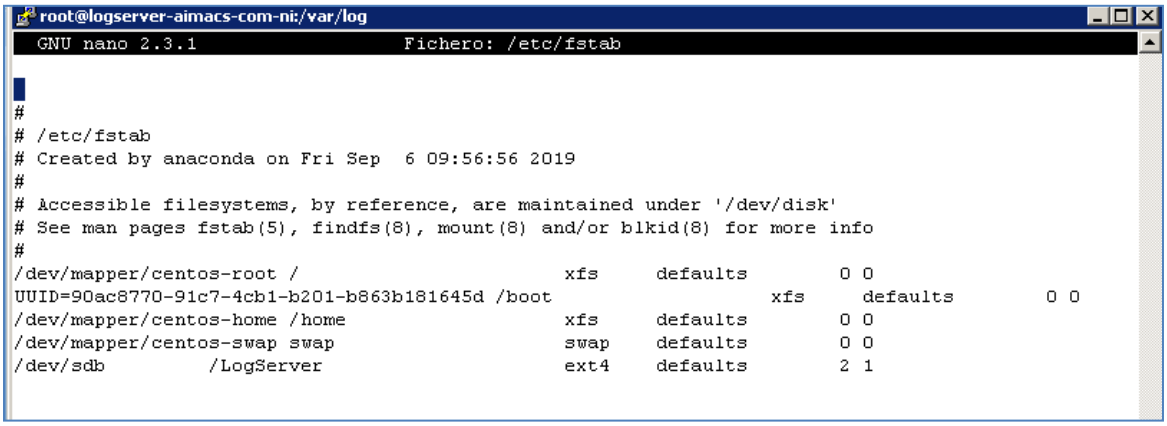
Luego Modificamos el archivo fstab para agregar el nuevo disco en el arranque con:

nano /etc/fstab

agregando la línea:

/dev/sdb /LogServer ext4 defaults 2 1

Tal como se muestra en la imagen siguiente:



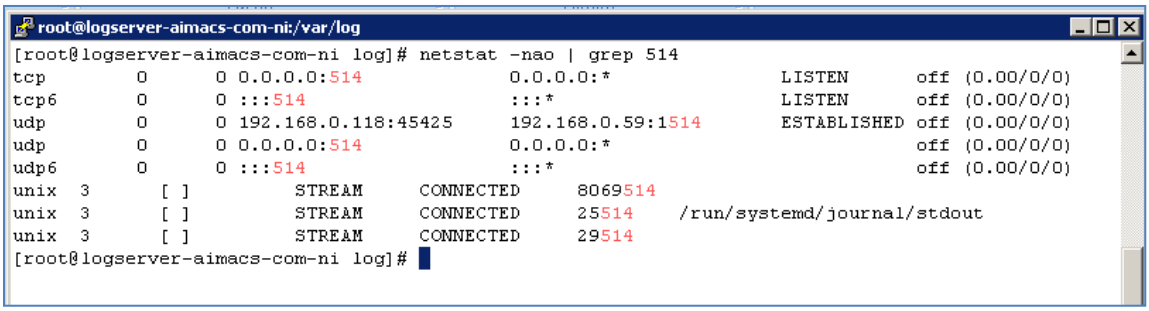
Montamos la partición creada en la carpeta LogServer con el comando:

mount -t ext4 /dev/sdb /LogServer

Ahora lo que queda es verificar el uso del Puerto 514

netstat -nao | grep 514

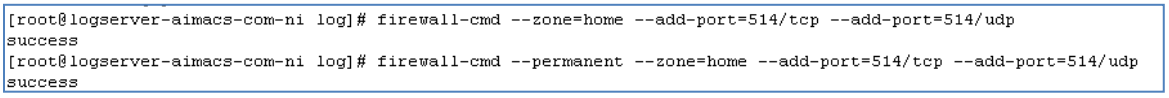
netstat -nao | grep syslog



Luego de tener verificado que rsyslog está instalado hay que proceder a generar reglas para iptables y para seelinux. Porque sino al momento de configurar el acceso al nuevo directorio de LOG no será posible. El comando firewall-cmd solo ve la parte del firewall y el comando semanage agrega permiso al puerto de syslog vía seelinux. Los comando ejecutados para dicha configuración son:

firewall-cmd --zone=home --add-port=514/tcp --add-port=514/udp
firewall-cmd --permanent --zone=home --add-port=514/tcp --add-port=514/udp

Como se observa los comandos son aplicados de forma satisfactoria en la siguiente imagen.



En el caso del seelinux se permite los puertos con propósito de LOG con los comandos siguientes:

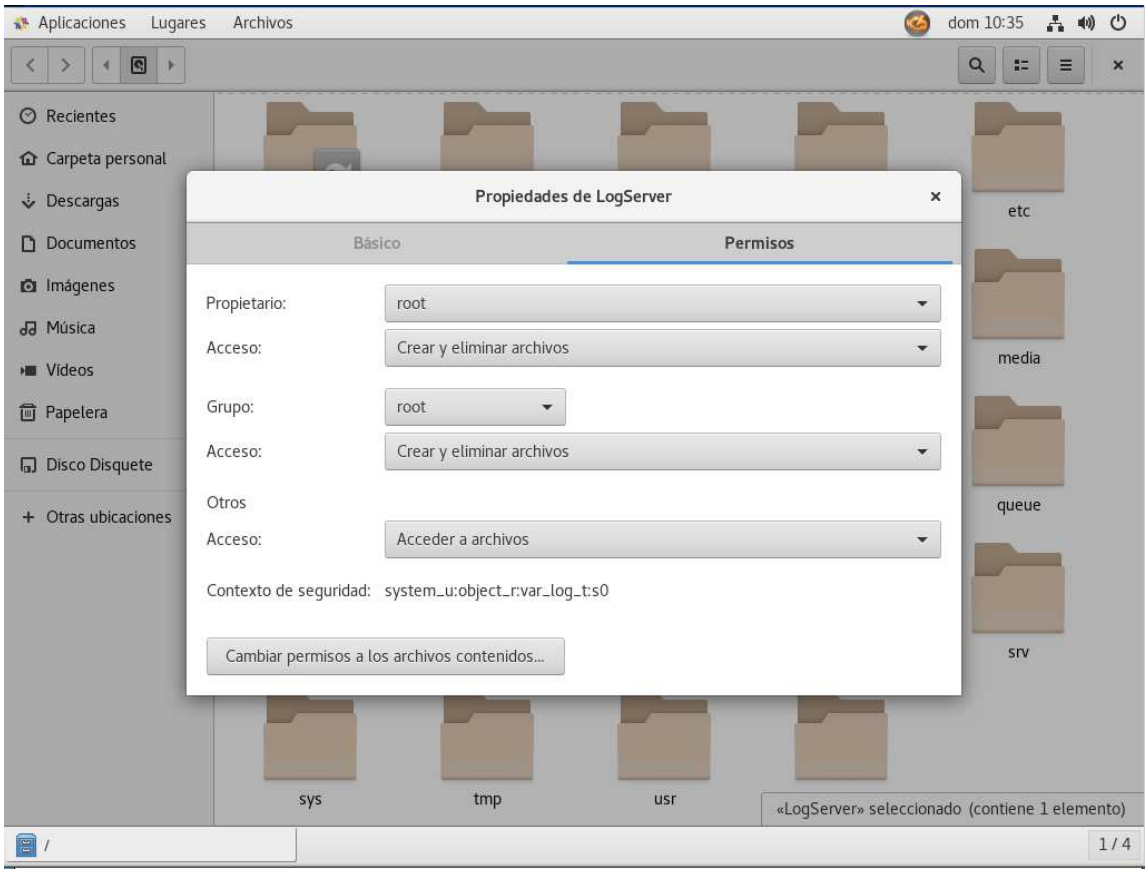
semanage port -a -t syslogd_port_t -p udp 514

semanage port -a -t syslogd_port_t -p tcp 514

Lo que ahora queda es asignar el mismo contexto de seelinux de la carpeta log a la nueva carpeta:

chcon --reference /var/log /LogServer/

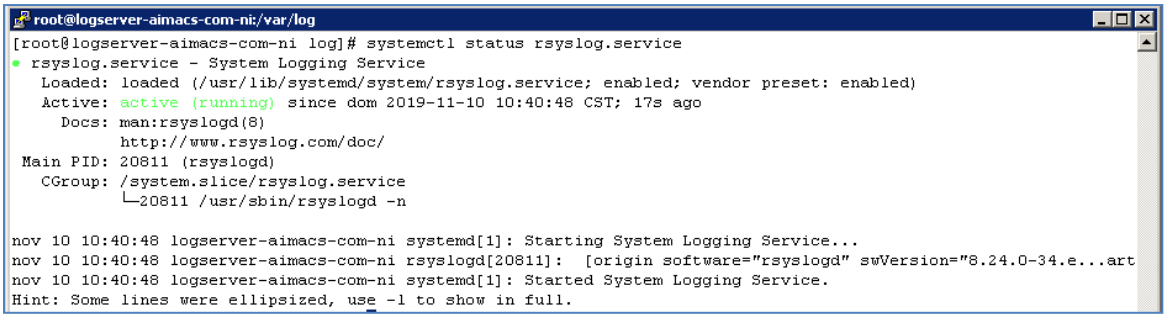
en la imagen que sigue se observará el contexto asignado a la carpeta LogServer.



Ahora ya estamos listos para configurar el servicio rsyslog. Lo primero es ver su estado actual. Lo hacemos con el comando:

systemctl status rsyslog.service

El resultado del comando es la imagen que sigue, que indica que el servicio está activo.



Lo que ahora queda es configurar adecuadamente el servicio ya que sólo fue instalado por defecto con el Centos7. Para eso editamos el archivo /etc/rsyslog.conf y quitamos comentarios a las siguientes líneas.

Provides UDP syslog reception

$ModLoad imudp

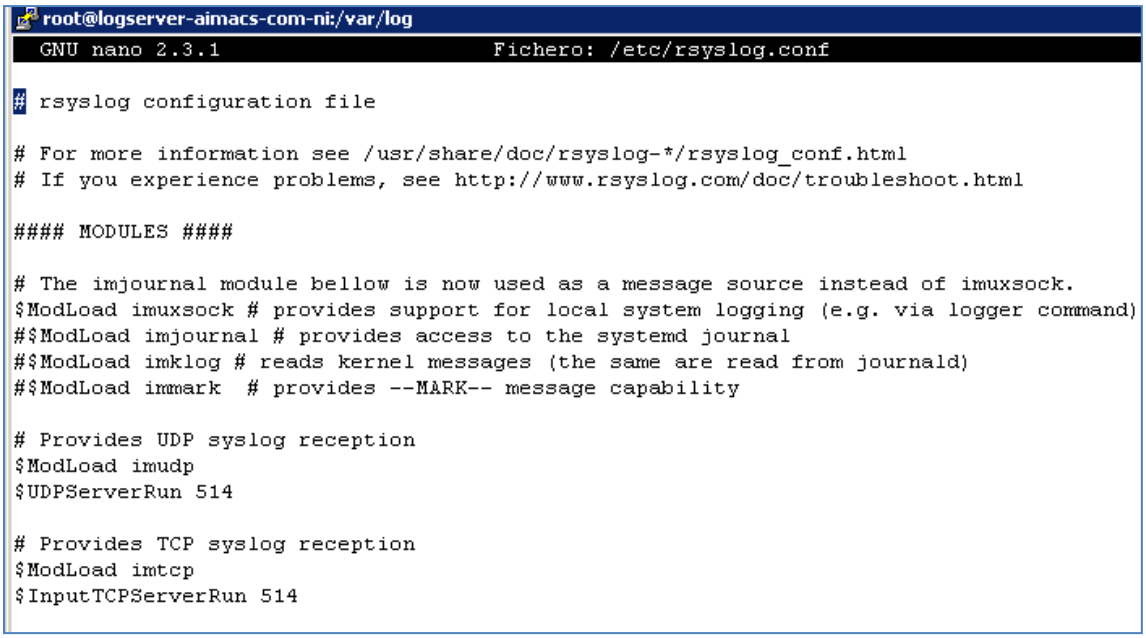
$UDPServerRun 514

Provides TCP syslog reception

$ModLoad imtcp

$InputTCPServerRun 514

La imagen que sigue muestra como queda configurada esta parte:



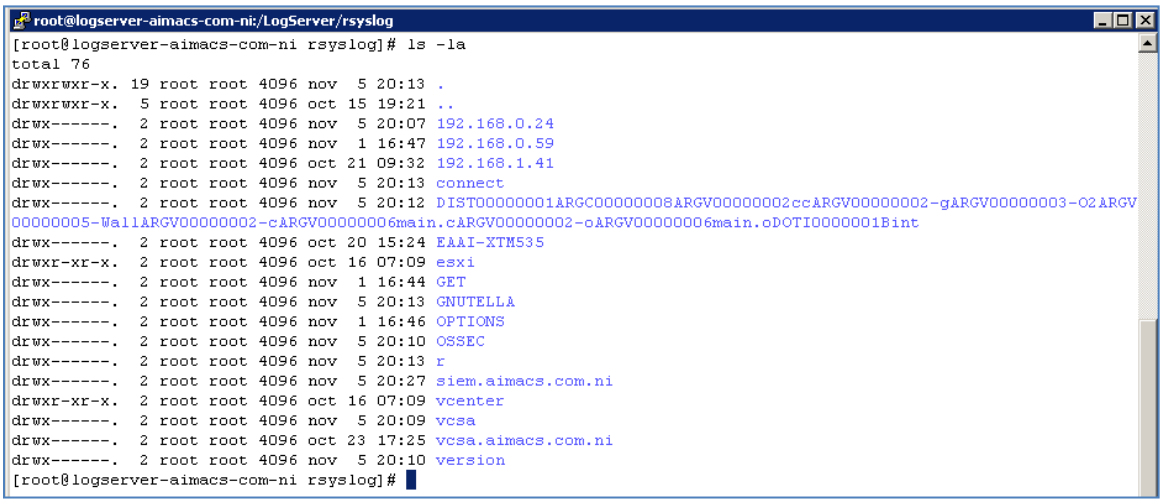
Lo anterior le permite al servicio rsyslog estar configurado para escuchar en los puertos tcp y udp 514.

La siguiente etapa del proceso es decirle a rsyslog donde guardar sus datos. Para esto en la parte de reglas (RULES) configuramos las siguientes líneas:

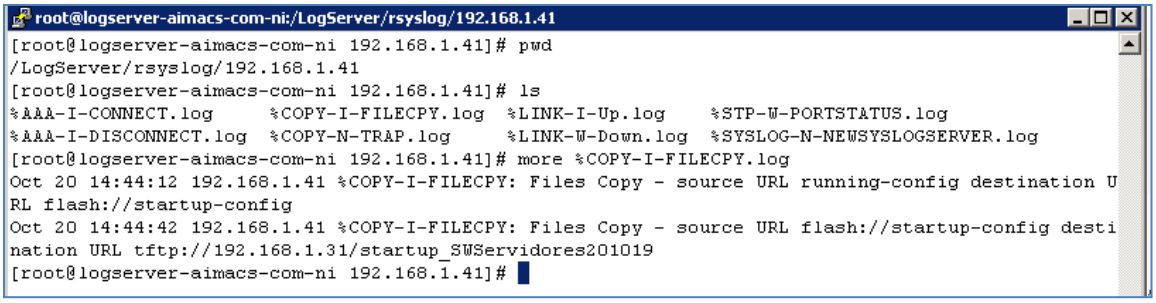
```
#### RULES ####
$CreateDirs on
$template TmplAuth, "/LogServer/rsyslog/%HOSTNAME%/%PROGRAMNAME%.log"
$template TmplMsg, "/LogServer/rsyslog/%HOSTNAME%/%PROGRAMNAME%.log"
authpriv.*  ?TmplAuth
*.*   ?TmplMsg
```

La siguiente imagen ilustra las líneas insertadas en el archivo de configuración. En este caso las que inician con $template son dos plantillas una llamada TmplAuth que recibiera todos los log que tienen que ver con autenticación y la otra llamada TmplMsg que recibirá cualquier LOG proveniente de equipos remotos. En la sintaxis se ilustra que después del nombre de la plantilla entre comillas se escribe la ruta de donde guardar los registros de eventos. Pero a demás se usan las variables %HOSTNAME% y %PROGRAMNAME%.log, la primera variable es la que se usa para crear una carpeta con el nombre del equipo remoto que se conecta al servidor de LOG, esto porque está activa la opción crear directorios $CreatDirs on, y la segunda es la que de cada equipo remoto va creando de forma dinámica los archivos de LOG.

Si observamos la carpeta LogServer y dentro de ella vamos a rsyslog que es la ruta base para guardar LOG podemos ver las carpetas de todos los dispositivos que se contactan ha ese equipo. La siguiente imagen nos muestran todos los equipos que están enviando sus LOG.



Si deseamos entrar para comprobar LOG de algún equipo solo buscamos la carpeta deseada por ejemplo 192.168.1.41 y listamos los archivos. Luego seleccionamos el que deseamos ver y lo leemos con el comando more. Ver la siguiente imagen.



Como se puede observar se ha podido leer sin problemas los LOG enviados y así cada equipo nos da información valiosa que puede gestionarse con este servidor.

A-8. Proceso de Aprobación de Piloto SIEM

Para iniciar la implementación y estudio del SIEM en la EAAI se realizó la siguiente solicitud:

SOLICITUD DE EJECUCIÓN DE TESIS

03 de mayo de 2019

Msc. Juan Ernesto Aguilar Narvaez
Gerente de TI

Por medio de la presente solicito apoyo para desarrollo final de tesis que pretende solventar uno de los principales problemas que actualmente enfrenta la EAAI en materia de seguridad; esto es la gestión del volumen disperso de información generado por los diferentes equipos de seguridad (Switches, Routers, UTM, Administrador de Ancho de banda) y Servidores

La Tesis que estoy finalizando de la Maestría en Gestión de la Seguridad de la Información (MGSI) lleva por título:

IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO DE EVENTOS DE SEGURIDAD EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA EMPRESA ADMINISTRADORA DE AEROPUERTOS INTERNACIONALES (EAAI)

Este proyecto tiene por propósito contribuir a la EAAI a tener visibilidad de su infraestructura tecnológica; puesto que la gran cantidad de registros de seguridad que generan los equipos de la infraestructura tecnológica poseen información valiosa para identificar ataques y comportamientos anómalos dentro de la red de la empresa. En el desarrollo de este trabajo se podrá observar el proceso de identificación y selección del software SIEM a utilizar; se identificará del mercado actual tanto las características comparativas como los costos asociados y sus beneficios de un grupo reducido de software SIEM; esto de acuerdo a los software más destacados en el cuadrante Mágico de Gartner. Durante todo el trabajo se analizarán las necesidades de procesamiento y almacenamiento de la empresa y se brindará recomendación de cual solución es más factible. Cabe mencionar que el software a implementar será un producto con licencia de carácter temporal (Demo, Trial).

Agradeciendo de antemano su apoyo.

Ing. Diego Manuel Vega Amoretti

Respuesta obtenida página 1/2:

Gobierno de Reconciliación y Unidad Nacional
El Pueblo, Presidente!
2019
Aquí nos ilumina, un Sol que no declina
El Sol que alumbra las nuevas victorias
RUBÉN DARÍO

EMPRESA ADMINISTRADORA DE AEROPUERTOS INTERNACIONALES
Gerencia de Tecnología de Información

MEMORANDUM
GTI-0140-2019

A : Ing. Diego Vega

DE : Ing. Juan Ernesto Aguilar
Gerente T.I

REF. : Autorización para implementar proyecto SIEM

FECHA: 14 de junio de 2019

Por medio de la presente le notifico la autorización de la Gerencia de TI del desarrollo de la **Tesis de Maestría** con el título: **IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO DE EVENTOS DE SEGURIDAD EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA EMPRESA ADMINISTRADORA DE AEROPUERTOS INTERNACIONALES (EAAI)**.Esto producto del reconocimiento de la importancia que genera la implementación de un SIEM para la obtención de visibilidad de la red de la empresa.

Debido a que este desarrollo es con fines didácticos y por superación profesional no se permitirá hacer uso de toda la infraestructura de la EAAI. Se limitará a utilizar los equipos de backup para pruebas y se proveerá conexión a puerto espejo que genere información del Router principal en la WAN y la traslade a un Router de backup para poder hacer cualquier configuración en esos tipos de equipos. Se proveerá una copia de los LOG de uno de los UTM. No se permitirá el acceso bajo ninguna circunstancia a los servidores de correos y DNS. Se permitirá una copia del controlador de dominio en un equipo virtual para instalar cualquier agente requerido por el SIEM. A demás se proveerá la infraestructura virtual requerida para implementar el SIEM y cualquier equipo extra requerido por la misma.

FE, FAMILIA Y COMUNIDAD!
CRISTIANA, SOCIALISTA, SOLIDARIA!
EMPRESA ADMINISTRADORA DE AEROPUERTOS INTERNACIONALES
Km.11 Carretera Norte/2276-9180-.2276-9280/www.eaai.com.ni

Respuesta obtenida página 2/2:

Gobierno de Reconciliación y Unidad Nacional
El Pueblo, Presidente!
2019
Aquí nos ilumina, un Sol que no declina
El Sol que alumbra las nuevas victorias
RUBÉN DARÍO

Cabe mencionar que este proceso ha sido aprobado hasta este tiempo por la falta de recursos de hardware disponibles y por el hecho que hasta esta fecha contamos con un sistema de vitalización con disponibilidad para su proyecto.

Para nosotros como empresa estas pruebas de implementación se tendrán como un piloto de lo que posteriormente se implementará en gran escala.

Esperamos que tenga éxito en el proceso.

Sin mas a que hacer referencia, me suscribo.

UNID@S EN VICTORIAS!
Por Gracia de Dios!

FE, FAMILIA Y COMUNIDAD!
CRISTIANA, SOCIALISTA, SOLIDARIA!
EMPRESA ADMINISTRADORA DE AEROPUERTOS INTERNACIONALES
Km.11 Carretera Norte/2276-9180-.2276-9280/www.eaai.com.ni

Resultados del piloto de implementación de SIEM:

Gobierno de Reconciliación y Unidad Nacional
El Pueblo, Presidente!
2019
Aquí nos ilumina, un Sol que no declina
El Sol que alumbra las nuevas victorias
RUBÉN DARÍO

EMPRESA ADMINISTRADORA DE AEROPUERTOS INTERNACIONALES
Gerencia de Tecnología de Información

M E M O R A N D U M
GTI-00301-2019
A : Ing. Diego Vega.

DE : Ing. Juan Ernesto Aguilar
Gerente TI

REF. : Evaluación de SIEM implementado

FECHA: 11 de noviembre de 2019

Por medio de la presente notifico mi conformidad como Gerente de TI del proyecto piloto que se desarrollo bajo el titulo de Maestria: **IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO DE EVENTOS DE SEGURIDAD EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA EMPRESA ADMINISTRADORA DE AEROPUERTOS INTERNACIONALES (EAAI).**

Dicho proyecto ha venido a contribuir a mejorar la visibilidad de la infraestructura solo con la integración de algunos pequeños elementos como un UTM, Servidor de LOG, Router (Backup) y un Swich. Toda la información mostrada tanto en el proceso de búsqueda de versiones como la implementación y selección del software SIEM OSSIM por cuestiones de factibilidad económica nos ha parecido excelente. Sabemos que el software por no ser la versión de paga tiene ciertas limitantes como la gestión directa de los LOG en brutos y la capacidad de almacenar los mismos. Pero resulta sumamente provechoso el tener una herramienta que te almacene al menos un mes de información transcendental y que permita correlacionar todo lo que ocurre. Esto para nosotros nos da la pauta que podemos utilizar el proyecto piloto y ampliarlo a mas niveles (incluir equipos vitales y toda la red).

Esperamos muy pronto iniciemos en enero del año que viene este proyecto y si es posible combinar con el otro software llamado SPLUNK.
Agradeciendo la contribución le saluda.

Sin más a que hacer referencia, me suscribo.

Atentamente,

Cc.: Archivo.

FE, FAMILIA Y COMUNIDAD!
CRISTIANA, SOCIALISTA, SOLIDARIA!
EMPRESA ADMINISTRADORA DE AEROPUERTOS INTERNACIONALES
Km.11 Carretera Norte/2276-9180-.2276-9280/www.eaai.com.ni

A-9. Modelo de Gestión de Evento

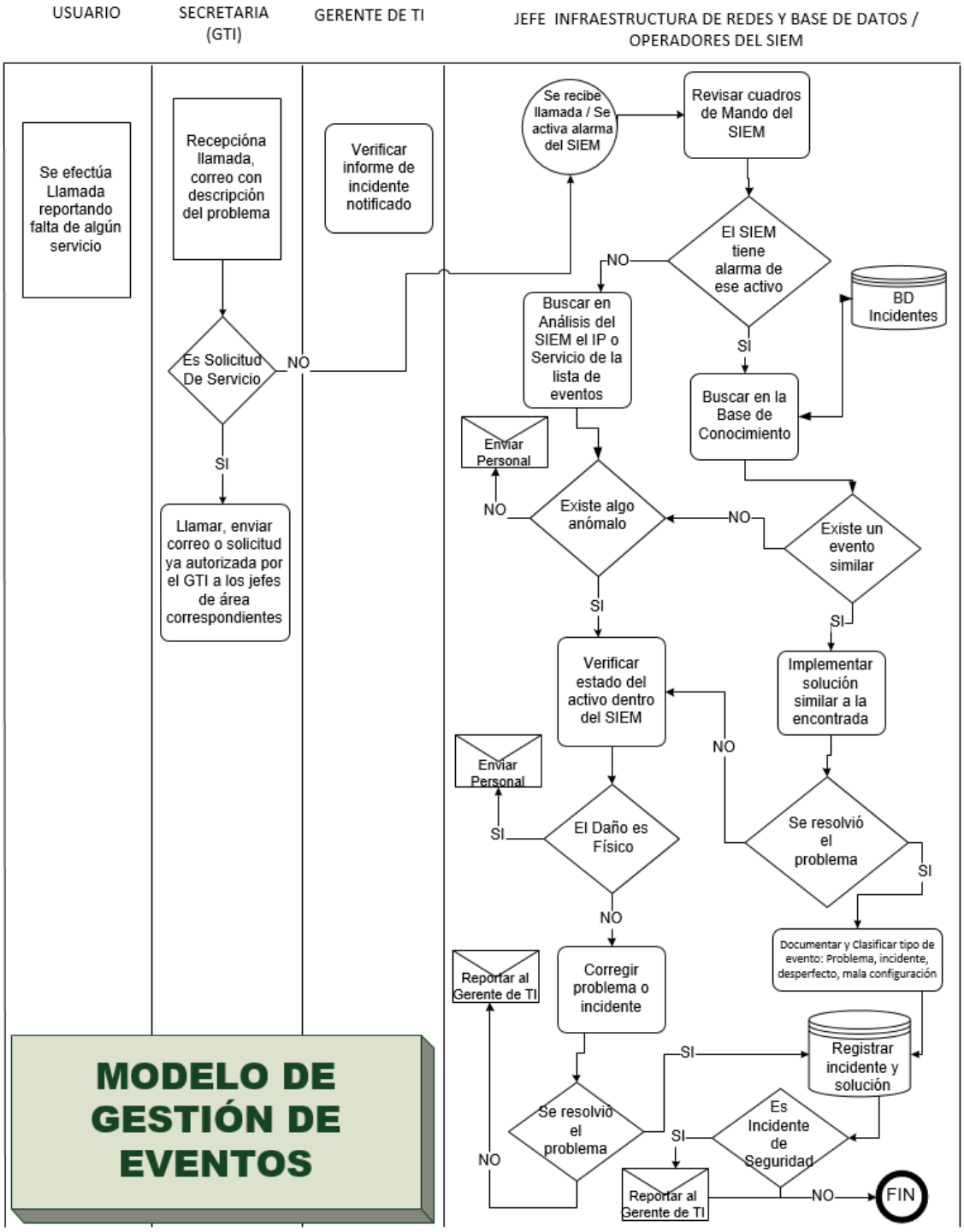
A continuación se describe en forma general el diagrama que se muestra en la siguiente página que es el modelo de gestión de eventos propuesto para la EAAI. Lo primero que se establece es la división del trabajo por tres áreas sin incluir al usuario. La Secretaria, Gerente de TI, Jefe de Infraestructura de redes y bases de datos y Operadores del SIEM. El diagrama de flujo indica que todo incidente puede ser reportado por un usuario a la secretaria directamente. Será la secreataria la encargada de enviar el requerimiento al Jefe de infraestructura. Cuado el área de infraestructura que administra el SIEM recibe el requerimiento para evaluar el problema se procede de la siguiente forma:

- Se debe verificar los cuadros de mando del SIEM.
- Se pregunta si el SIEM tiene alarma de ese activo. De ser verdadero hace lo siguiente:
    - Buscar en la base de conocimientos si existe un evento similar registrado.
    - Implementa una solución similar.
    - Si el problema se resuelve se documenta y clasifica. En este punto se define la forma en que clasificamos los eventos ocurridos. Ej. Evento de seguridad, evento, incidente, mala configuración, etc.
    - Luego se procede a registrar el detalle de todo lo realizado.
    - Se verifica si es un evento de seguridad. De ser así se envía correo al Gerente de TI para que esté enterado de lo ocurrido.
    - Si fue algo no relevante solo se cierra el caso registrado.
- En caso que el SIEM no tenga alarma se procede de la siguiente forma:
    - De los eventos generados por el SIEM y ubicados en análisis se debe validar si existe algún comportamiento anómalo o poco común detectado en los equipos fuentes. Si no existe se envía personal técnico al lugar del activo con problemas.
    - Si se nota alguna anomalía se procede a verificar el estado del activo dentro del SIEM.

  - Se verifica si el daño es físico. De ser físico se envía personal
  - Si el problema no se resuelve se envía notificación al Gerente de TI.
  - Si el problema se resuelve se registra en al BD de incides.
  - Se valida si el incidente clasificado era de seguridad o cualquier otro. De ser de seguridad se envía correo al Gerente de TI.
- Concluye el proceso

Cabe mencionar que la empresa para los registros de solicitudes e incidentes tiene distintos tipos de formatos y almacenamientos. Actualmente está en etapa de desarrollo de un software para gestión de servicios de TI o mesa de ayuda. Este software servirá como base de conocimiento de todo incidente o servicio registrado en la empresa. Pero para poder seguir el diagrama que sigue mas adelante es necesario que la empresa haga uso de algún software de gestión de recursos de TI o Help Desk que permita a todo el personal compartir problemas, casos, incidentes y cualquier requerimiento de usuario en un solo lugar.

A continuación en la siguiente página se mostrará el diagrama de modelo de eventos.


USUARIO
SECRETARIA (GTI)
GERENTE DE TI
JEFE INFRAESTRUCTURA DE REDES Y BASE DE DATOS / OPERADORES DEL SIEM
Se efectúa Llamada reportando falta de algún servicio
Recepcióna llamada, correo con descripción del problema
Verificar informe de incidente notificado
Se recibe llamada / Se activa alarma del SIEM
Revisar cuadros de Mando del SIEM
El SIEM tiene alarma de ese activo
NO
SI
BD Incidentes
Buscar en Análisis del SIEM el IP o Servicio de la lista de eventos
Buscar en la Base de Conocimiento
Es Solicitud De Servicio
NO
SI
Llamar, enviar correo o solicitud ya autorizada por el GTI a los jefes de área correspondientes
Enviar Personal
NO
Existe algo anómalo
NO
Existe un evento similar
SI
SI
Verificar estado del activo dentro del SIEM
Implementar solución similar a la encontrada
Enviar Personal
NO
SI
El Daño es Físico
Se resolvió el problema
SI
NO
Documentar y Clasificar tipo de evento: Problema, incidente, desperfecto, mala configuración
Reportar al Gerente de TI
Corregir problema o incidente
Registrar incidente y solución
SI
Se resolvió el problema
Es Incidente de Seguridad
SI
NO
Reportar al Gerente de TI
NO
FIN
MODELO DE GESTIÓN DE EVENTOS